

1 I, Richard R. Wiebe, do hereby declare:

2 1. I am a member in good standing of the Bar of the State of California and the bar of
3 this Court. I am counsel to plaintiffs in this action.

4 2. Attached hereto as **Exhibit A** is a true and correct copy of Danny Yadron and Evan
5 Perez, *T-Mobile, Verizon Wireless Shielded from NSA Sweep*, Wall St. J. (June 14, 2013); *available*
6 *at*: <http://online.wsj.com/news/articles/SB10001424127887324049504578543800240266368>.

7 3. Attached hereto as **Exhibit B** is a true and correct copy of Barton Gellman, *U.S.*
8 *surveillance architecture includes collection of revealing Internet, phone metadata*, Wash. Post
9 (June 14, 2013); *available at*: [http://www.washingtonpost.com/investigations/us-surveillance-](http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html)
10 [architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-](http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html)
11 [11e2-b05f-3ea3f0e7bb5a_story.html](http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html).

12 4. Attached hereto as **Exhibit C** is a true and correct copy of Jennifer Valentino-
13 DeVries and Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA*
14 *Data-Gathering*, Wall St. J. (July 8, 2013); *available at*:
15 <http://online.wsj.com/news/articles/SB10001424127887323873904578571893758853344>.

16 5. Attached hereto as **Exhibit D** is a true and correct copy of Primary Order, In re
17 Application of the Federal Bureau of Investigation for an Order Requiring the Production of
18 Tangible Things from [Redacted], No. BR 11-07 (FISC Jan. 20, 2011).

19 6. Attached hereto as **Exhibit E** is a true and correct copy of a January 27, 2014 letter
20 from Deputy Attorney General James M. Cole to Facebook, Google, LinkedIn, Microsoft, and
21 Yahoo.

22 7. Attached hereto as **Exhibit F** is a true and correct copy of Cecilia Kang and Ellen
23 Nakashima, *Tech executives to Obama: NSA spying revelations are hurting business*, Wash. Post
24 (Dec. 17, 2013); *available at*: [http://www.washingtonpost.com/business/technology/tech-](http://www.washingtonpost.com/business/technology/tech-executives-to-obama-nsa-spying-revelations-are-threatening-business/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html)
25 [executives-to-obama-nsa-spying-revelations-are-threatening-business/2013/12/17/6569b226-6734-](http://www.washingtonpost.com/business/technology/tech-executives-to-obama-nsa-spying-revelations-are-threatening-business/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html)
26 [11e3-a0b9-249bbb34602c_story.html](http://www.washingtonpost.com/business/technology/tech-executives-to-obama-nsa-spying-revelations-are-threatening-business/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html).

27 8. Attached hereto as **Exhibit G** is a true and correct copy of Associated Press, *Tech*
28 *industry: Obama's NSA reforms 'insufficient,'* Wash. Post (Jan. 18, 2014); *available at*:

1 [http://www.washingtonpost.com/business/tech-industry-obamas-nsa-reforms-
insufficient/2014/01/18/1a8f1a7e-8071-11e3-97d3-b9925ce2c57b_story.html](http://www.washingtonpost.com/business/tech-industry-obamas-nsa-reforms-
2 insufficient/2014/01/18/1a8f1a7e-8071-11e3-97d3-b9925ce2c57b_story.html).

3 9. Attached hereto as **Exhibit H** is a true and correct copy of Craig Timberg, Barton
4 Gellman and Ashkan Soltani, *Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its*
5 *Internet traffic*, Wash. Post (Nov. 26, 2013); *available at:*

6 [http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-
up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-
caf30787c0a9_story.html](http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-
7 up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-
8 caf30787c0a9_story.html).

9 I declare under penalty of perjury under the laws of the United States that the foregoing is
10 true and correct to the best of my knowledge, information, and belief.

11 Executed at San Francisco, CA on January 31, 2014.

12 _____
13 *s/ Richard R. Wiebe*

14 Richard R. Wiebe
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT A

News, Quotes, Companies, Videos **SEARCH**

SUBSCRIBE NOW and get **3 MONTHS** for the **PRICE OF 1** **SUBSCRIBE NOW**

U.S. EDITION Friday, June 14, 2013 As of 11:21 AM EDT

[Subscribe](#) | [Log In](#)

[Home](#) [World](#) **[U.S.](#)** [New York](#) [Business](#) [Tech](#) [Markets](#) [Market Data](#) [Opinion](#) [Life & Culture](#) [Real Estate](#) [Management](#) [C-Suite](#)
[Seib & Wessel](#) [Politics & Policy](#) [Washington Wire](#) [Budget Battle](#) [Economy](#) [San Francisco Bay Area](#) [WSJ/NBC News Poll](#) [Journal Report](#) [Columns & Blogs](#)

TOP STORIES IN POLITICS

10 of 12

[Companies Push Back on Demands for Data](#)

11 of 12

[Cuomo's Marijuana Decriminalization Push Likely Dead for This Year](#)



[Blind Chinese Dissident to Leave NYU](#)

12 of 12



[U.S. to Arm Syr Rebels](#)

POLITICS | Updated June 14, 2013, 11:21 a.m. ET

T-Mobile, Verizon Wireless Shielded from NSA Sweep

Article

Stock Quotes

Comments (20)

MORE IN POLITICS & POLICY >

Email

Print



By [DANNY YADRON](#) and [EVAN PEREZ](#)

WASHINGTON—The National Security Agency's controversial data program, which seeks to stockpile records on all calls made in the U.S., doesn't collect information directly from T-Mobile USA and Verizon Wireless, in part because of their foreign ownership ties, people familiar with the matter said.

The blind spot for U.S. intelligence is relatively small, according to a U.S. official. Officials believe they can still capture information, or metadata, on 99% of U.S. phone traffic because nearly all calls eventually travel over networks owned by U.S. companies that work with the NSA.



Enlarge Image

Bloomberg News

Retired Adm. Mike Mullen is expected to fill a new board-level position of security director at Japan's Softbank Corp. after Softbank's acquisition of Sprint.

Nonetheless, the decision to exclude companies with overseas ties could present future challenges for the U.S. government as long as such investors continue to play a large role in operating the country's telecom infrastructure. The nation's other two nationwide wireless carriers, [AT&T Inc.](#) T -0.72% and [Sprint Nextel Corp.](#), S +2.32% have long cooperated with the government, people familiar with the matter said.

T-Mobile and Verizon Wireless don't participate in their own collection programs because of legal complications stemming, in part, from their foreign ownership. Germany's [Deutsche Telekom AG](#) DTE.XE -0.19% owns 74% of T-Mobile. Verizon Wireless is a joint-venture of [Verizon Communications Inc.](#) VZ +0.93% with the U.K.'s [Vodafone Group](#) VOD.LN +0.76% PLC, which owns a 45% stake.

Japan's [SoftBank Corp.](#) 9984.TO +1.20% is pushing to complete an acquisition of Sprint by July. In order for the company to engage in other classified activities with the U.S., it is expected to create a separate U.S. subsidiary. It would also create a new board-level position of security director, set to be filled by retired Adm. [Mike Mullen](#), former chairman of the Joint Chiefs of Staff.

The exclusion of T-Mobile and Verizon Wireless from the sprawling domestic surveillance program underscores the deep ties the U.S. telecom industry

THE NEW PORTFOLIO TOOL ON WSJ.COM:
ENTER YOUR BROKERAGE ACCOUNT DETAILS.
WE'LL GIVE YOU ALL THE NEWS AND INFO YOU NEED.
[LEARN MORE](#)
provided by LikeAssets

Available to WSJ.com Subscribers

[Patients Put at Risk By Computer Viruses](#)



[Refinancings Plunge as Bond Yields Rise](#)

[Behind the Profits: A Tax Break](#)

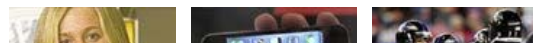
[Foreign Stakes Shield Two Phone Firms from NSA Sweep](#)



GET 3 MONTHS FOR THE PRICE OF 1 [SUBSCRIBE NOW](#)

Don't Miss

[?]



maintains with the U.S. intelligence world.

The NSA program, which requires a warrant granted by a secret court, permits the agency to record numbers, length and location of every call from the participating carriers. President [Barack Obama](#) has said that the NSA doesn't monitor conversations.

Legal, practical and political obstacles are all possible reasons why the two firms are excluded from the NSA program. But current and former U.S. officials say the likely reasons are tied to their overseas ownership. Government requests for data, through special court orders sanctioned by the Foreign Intelligence Surveillance Act, are classified "top secret" and "noforn," spy-talk for "no foreign." That would prohibit some T-Mobile and Verizon owners from being aware of the programs.

Unlike Sprint and AT&T, the two wireless firms also don't perform classified work for the government. Such contracts require secure facilities that make cooperating with NSA programs simpler, people familiar with the matter said.

Much of the U.S.'s telecom backbone is owned by two companies: AT&T and Verizon Business Network Services Inc., a U.S. subsidiary of Verizon Communications that it views as a separate network from its mobile business. It was the Verizon subsidiary that was named in the FISA warrant leaked by NSA contractor Edward Snowden to the Guardian newspaper and revealed last week.

When a T-Mobile or Verizon Wireless call is made, it often must travel over one of these networks, requiring the carrier to pay the cable owner. The information related to that transaction—such as the phone numbers involved and length of call—is recorded and can then be passed to the NSA through its existing relationships. Additionally, T-Mobile relies on other wireless companies to fill holes in its infrastructure. That shared equipment could allow the government to collect the data.

The NSA has standing court orders with AT&T and Sprint for information on all calls over their networks within, into and out of the U.S., according to people familiar with the matter.

U.S. companies, including Verizon Wireless and T-Mobile, are required to comply with warrants and court orders relating to standard criminal probes. In 2011, Verizon Wireless received 260,000 requests for customer data, according to a letter it sent last year to Rep. Edward Markey (D., Mass.). The company said about half were in the form of warrants or court orders.

In this instance, U.S. officials appear to be making a deliberate choice to not start the more-sensitive and expansive NSA collection programs with the two wireless carriers.

—Anton Troianovski contributed to this article.

Write to Danny Yadron at danny.yadron@wsj.com and Evan Perez at evan.perez@wsj.com

A version of this article appeared June 14, 2013, on page A4 in the U.S. edition of The Wall Street Journal, with the headline: Foreign Stakes Shield Firms From NSA Sweep.

JOIN THE DISCUSSION
20 Comments, add yours

MORE IN
Politics & Policy »

Email Print Order Reprints



Meet Bu... Privacy Issue: All...
28-Year-Old... Web... Losing...
Executive Demands No... Fluke...
Phone

Watch NFL Games on Your (Verizon) Phone

U.S. to Arm Syrian Rebels



U.S. Military Proposal to Arm Rebels Includes No-Fly Zone...

Opinion: Surveillance and Its Discontents



5 Refinancings Plunge as Bond Yields Rise

Show 5 More

Real-time Washington News and Insight

Seib & Wessel: What We're Reading Friday

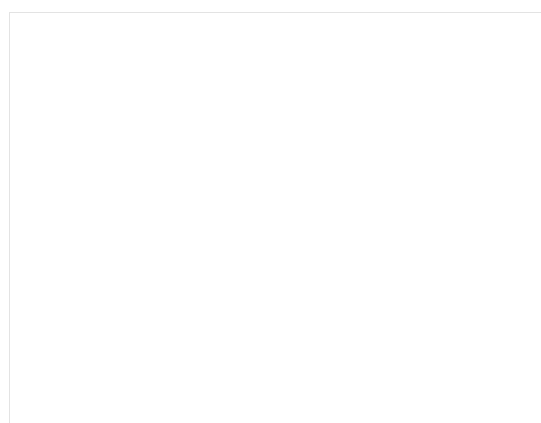
A look ahead to Bernanke's press conference next week, the difficulty of reconciling U.S. humanitarian ideals, and more recommended reading from around the web.



Arizona Expands Medicaid in Win for Gov. Brewer

White House Statement on Use of Chemical Weapons in Syria

See All
RSS Feed



THE NEW PORTFOLIO TOOL ON WSJ.COM:
ENTER YOUR BROKERAGE ACCOUNT DETAILS.
WE'LL GIVE YOU ALL THE NEWS AND INFO YOU NEED.

LEARN MORE

provided by LikeAssets

EXHIBIT B

The Washington Post

[Back to previous page](#)

U.S. surveillance architecture includes collection of revealing Internet, phone metadata

By Barton Gellman, Published: June 15

On March 12, 2004, [acting attorney general James B. Comey](#) and the Justice Department's top leadership reached the brink of resignation over electronic surveillance orders that they believed to be illegal.

President George W. Bush backed down, halting secret foreign-intelligence-gathering operations that had crossed into domestic terrain. That morning marked the beginning of the end of STELLARWIND, the cover name for a set of four surveillance programs that brought Americans and American territory within the domain of the [National Security Agency](#) for the first time in decades. It was also a prelude to new legal structures that allowed Bush and then President Obama to reproduce each of those programs and expand their reach.

What exactly STELLARWIND did has never been disclosed in an unclassified form. Which parts of it did Comey approve? Which did he shut down? What became of the programs when the crisis passed and Comey, now Obama's expected nominee for FBI director, returned to private life?

Authoritative new answers to those questions, drawing upon a classified NSA history of STELLARWIND and interviews with high-ranking intelligence officials, offer the clearest map yet of the [Bush-era programs](#) and the NSA's contemporary U.S. operations.

STELLARWIND was succeeded by four major lines of intelligence collection in the territorial United States, together capable of spanning the full range of modern telecommunications, according to the interviews and documents.

Foreigners, not Americans, are the NSA's "targets," as the law defines that term. But the programs are structured broadly enough that they touch nearly every American household in some way. [Obama administration officials](#) and career intelligence officers say Americans should take comfort that privacy protections are built into the design and oversight, but they are not prepared to discuss the details.

The White House, the NSA and the Office of the Director of National Intelligence declined to comment on the record for this article. A senior intelligence official agreed to answer questions if not identified.

"We have rich oversight across three branches of government. I've got an [inspector general] here, a fairly robust legal staff here . . . and there's the Justice Department's national security division," the official said.

“For those things done under court jurisdiction, the courts are intrusive in my business, appropriately so, and there are two congressional committees. It’s a belts-and-suspenders-and-Velcro approach, and inside there’s rich auditing.”

But privacy advocates, such as [Sen. Ron Wyden \(D-Ore.\)](#), said the intelligence committee on which he serves needs “straight answers” to do vigorous oversight.

He added: “The typical person says, ‘If I am law-abiding and the government is out there collecting lots of information about me — who I call, when I call, where I call from’ . . . I think the typical person is going to say, ‘That sure sounds like it could have some effect on my privacy.’”

Two of the four collection programs, one each for telephony and the Internet, process trillions of “metadata” records for storage and analysis in systems called [MAINWAY](#) and MARINA, respectively. [Metadata](#) includes highly revealing information about the times, places, devices and participants in electronic communication, but not its contents. The bulk collection of telephone call records from [Verizon Business Services](#), disclosed this month by the British newspaper the Guardian, is one source of raw intelligence for MAINWAY.

The other two types of collection, which operate on a much smaller scale, are aimed at content. One of them intercepts telephone calls and routes the spoken words to a system called NUCLEON.

For Internet content, the most important source collection is the [PRISM project](#) reported on June 6 by The Washington Post and the Guardian. It draws from data held by [Google, Yahoo, Microsoft and other Silicon Valley giants](#), collectively the richest depositories of personal information in history.

Former [NSA contractor Edward Snowden](#), 29, who unmasked himself as the source behind the [PRISM](#) and Verizon revelations, said he hoped for a systematic debate about the “[danger to our freedom and way of life](#)” posed by a surveillance apparatus “kept in check by nothing more than policy.”

For well over a week, he has had his wish. Startling disclosures have poured out of the nation’s largest and arguably tightest-lipped spy agency at an unprecedented pace. Snowden’s disclosures have opened a national conversation about the limits of secret surveillance in a free society and an [outcry overseas against U.S. espionage](#).

The debate has focused on two of the four U.S.-based collection programs: [PRISM](#), for Internet content, and the comprehensive collection of telephone call records, foreign and domestic, that the Guardian revealed by posting a classified order from the Foreign Intelligence Surveillance Court to Verizon Business Services.

The Post has learned that similar orders have been renewed every three months for other large U.S. phone companies, including Bell South and AT&T, since May 24, 2006. On that day, the surveillance court made a fundamental shift in its approach to Section 215 of the Patriot Act, which permits the FBI to compel production of “business records” that are relevant to a particular terrorism investigation and to share those in some circumstances with the NSA. Henceforth, the court ruled, it would define the relevant business records as the entirety of a telephone company’s call database.

The Bush administration, by then, had been taking “bulk metadata” from the phone companies under voluntary agreements for more than four years. The volume of information overwhelmed the MAINWAY database, according to a classified report from the NSA inspector general in 2009. The agency spent \$146 million in supplemental counterterrorism funds to buy new hardware and contract support — and to make unspecified payments to the phone companies for “collaborative partnerships.”

When the New York Times revealed the warrantless surveillance of voice calls, in December 2005, the telephone companies got nervous. One of them, unnamed in the report, approached the NSA with a request. Rather than volunteer the data, at a price, the “provider preferred to be compelled to do so by a court order,”

the report said. Other companies followed suit. The surveillance court order that recast the meaning of business records “essentially gave NSA the same authority to collect bulk telephony metadata from business records that it had” under Bush’s asserted authority alone.

Telephone metadata was not the issue that sparked a rebellion at the Justice Department, first by Jack Goldsmith of the Office of Legal Counsel and then by Comey, who was acting attorney general because John D. Ashcroft was in intensive care with acute gallstone pancreatitis. It was Internet metadata.

At Bush’s direction, in orders prepared by David Addington, the counsel to Vice President Richard B. Cheney, the NSA had been siphoning e-mail metadata and technical records of Skype calls from data links owned by AT&T, Sprint and [MCI, which later merged with Verizon](#).

For reasons unspecified in the report, Goldsmith and Comey became convinced that Bush had no lawful authority to do that.

MARINA and the collection tools that feed it are probably the least known of the NSA’s domestic operations, even among experts who follow the subject closely. Yet they probably capture information about more American citizens than any other, because the volume of e-mail, chats and other Internet communications far exceeds the volume of standard telephone calls.

The NSA calls Internet metadata “digital network information.” Sophisticated analysis of those records can reveal unknown associates of known terrorism suspects. Depending on the methods applied, it can also expose medical conditions, political or religious affiliations, confidential business negotiations and extramarital affairs.

What permits the former and prevents the latter is a complex set of policies that the public is not permitted to see. “You could do analyses that give you more information, but the law and procedures don’t allow that,” a senior U.S. intelligence lawyer said.

In the urgent aftermath of Sept. 11, 2001, with more attacks thought to be imminent, analysts wanted to use “contact chaining” techniques to build what the NSA describes as network graphs of people who represented potential threats.

The legal challenge for the NSA was that its practice of collecting high volumes of data from digital links did not seem to meet even the relatively low requirements of Bush’s authorization, which allowed collection of Internet metadata “for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States,” the NSA inspector general’s report said.

Lawyers for the agency came up with an interpretation that said the NSA did not “acquire” the communications, a term with formal meaning in surveillance law, until analysts ran searches against it. The NSA could “obtain” metadata in bulk, they argued, without meeting the required standards for acquisition.

Goldsmith and Comey did not buy that argument, and a high-ranking U.S. intelligence official said the NSA does not rely on it today.

As soon as surveillance data “touches us, we’ve got it, whatever verbs you choose to use,” the official said in an interview. “We’re not saying there’s a magic formula that lets us have it without having it.”

When Comey finally ordered a stop to the program, Bush signed an order renewing it anyway. Comey, Goldsmith, FBI Director Robert S. Mueller III and most of the senior Bush appointees in the Justice Department began drafting letters of resignation.

Then-NSA Director Michael V. Hayden was not among them. According to the inspector general’s classified

report, Cheney's lawyer, Addington, placed a phone call and "General Hayden had to decide whether NSA would execute the Authorization without the Attorney General's signature." He decided to go along.

The following morning, when Mueller told Bush that he and Comey intended to resign, the president reversed himself.

Three months later, on July 15, the secret surveillance court allowed the NSA to resume bulk collection under the court's own authority. The opinion, which remains highly classified, was based on a provision of electronic surveillance law, known as "pen register, trap and trace," that was written to allow law enforcement officers to obtain the phone numbers of incoming and outgoing calls from a single telephone line.

When the NSA aims for foreign targets whose communications cross U.S. infrastructure, it expects to sweep in some American content "incidentally" or "inadvertently," which are terms of art in regulations governing the NSA. Contact chaining, because it extends to the contacts of contacts of targets, inevitably collects even more American data.

[Current NSA director Keith B. Alexander](#) and [Director of National Intelligence James R. Clapper Jr.](#) have resolutely refused to offer an estimate of the number of Americans whose calls or e-mails have thus made their way into content databases such as NUCLEON.

The agency and its advocates maintain that its protection of that data is subject to rigorous controls and oversight by Congress and courts. For the public, it comes down to a question of unverifiable trust.

"The constraints that I operate under are much more remarkable than the powers that I enjoy," said the senior intelligence official who declined to be named.

When asked why the NSA could not release an unclassified copy of its "minimization procedures," which are supposed to strip accidentally collected records of their identifying details, the official suggested a reporter submit a freedom-of-information request.

As for bulk collection of Internet metadata, the question that triggered the crisis of 2004, another official said the NSA is no longer doing it. When pressed on that question, he said he was speaking only of collections under authority of the surveillance court.

"I'm not going to say we're not collecting any Internet metadata," he added. "We're not using this program and these kinds of accesses to collect Internet metadata in bulk."

Julie Tate and Ellen Nakashima contributed to this report.

Sponsored Links

wheels when you want 'em.

Gas & insurance included. Join Zipcar now for \$50 free driving.
zipcar.com

What is Your Flood Risk?

Protect your home from floods. Get your flood risk profile today.
www.floodsmart.gov

TransUnion® Official Site

Get your credit score, and access powerful, tailored tools
transunion.com

[Buy a link here](#)

EXHIBIT C

\$1 A WEEK for 12 WEEKS SUBSCRIBE NOW

U.S. EDITION Monday, July 8, 2013 As of 3:13 AM EDT

Subscribe | Log In

Home World U.S. New York Business Tech Markets Market Data Opinion Life & Culture Real Estate Management C-Suite

Seib & Wessel Politics & Policy Washington Wire Budget Battle Economy WSJ/NBC News Poll Journal Report Columns & Blogs

TOP STORIES IN WSJ 1 of 12 Paul H. Robinson: Why the Zimmerman Verdict Will Be All 2 of 12 Barnes & Noble CEO Lynch Resigns 3 of 12 Pilot Error Eyed in Crash Best of the Web Today: 'Rape Culture' vs. 'Islamophobia'

U.S. NEWS Updated July 8, 2013, 3:13 a.m. ET

Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering

Article Video Stock Quotes Comments (229) MORE IN US >

Email Print

By JENNIFER VALENTINO-DEVRIES and SIOBHAN GORMAN

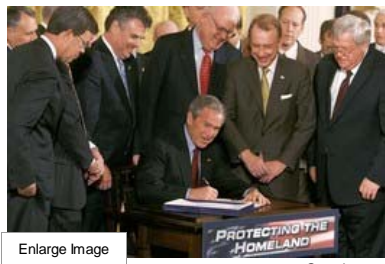
The National Security Agency's ability to gather phone data on millions of Americans hinges on a secret court ruling that redefined a single word: "relevant."



The National Security Agency's ability to gather phone data on millions of Americans hinges on the secret redefinition of the word "relevant." Jen Valentino-DeVries reports. Photo: Getty Images.

This change—which specifically enabled the surveillance recently revealed by former NSA contractor Edward Snowden—was made by the secret Foreign Intelligence Surveillance Court, a group of judges responsible for making decisions about government surveillance in national-security cases. In classified orders starting in the mid-2000s, the court accepted that "relevant" could be broadened to permit

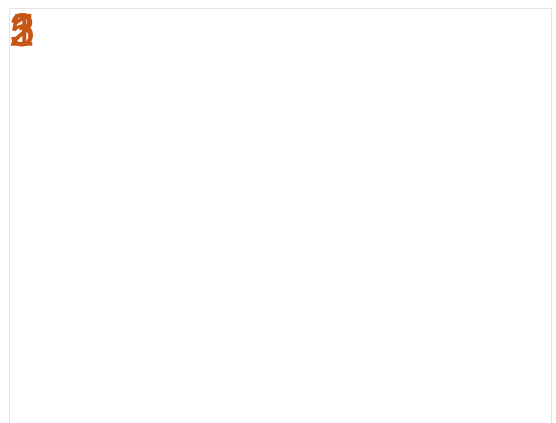
an entire database of records on millions of people, in contrast to a more conservative interpretation widely applied in criminal cases, in which only some of those records would likely be allowed, according to people familiar with the ruling.



The 'relevant' language was added to the Patriot Act when it came up for reauthorization; it was signed by President Bush in 2006.

In interviews with The Wall Street Journal, current and former administration and congressional officials are shedding new light on the history of the NSA program and the secret legal theory underpinning it. The court's interpretation of the word enabled the government, under the Patriot Act, to collect the phone records of the majority of Americans, including phone numbers people dialed and where they were calling from, as part of a continuing investigation into international terrorism.

"Relevant" has long been a broad standard, but the way the court is



THE NEW PORTFOLIO TOOL ON WSJ.COM: THE ULTIMATE INVESTMENT TRACKER AVAILABLE EXCLUSIVELY FOR SUBSCRIBERS LEARN MORE provided by LikeAssets

Available to WSJ.com Subscribers

Secret Ruling Expanded Spy Powers

From Permanent Resident to Citizen

Summers Circles as Fed Opening Looms

At 88, Former AIG

- Related Articles
Brazil Wants Explanation on Report of U.S. Surveillance
Nominee for FBI Top Post Likely to Face Tough Questions

interpreting it, to mean, in effect, "everything," is new, says Mark Eckenwiler, a senior counsel at Perkins Coie LLP who, until December, was the Justice Department's primary authority on federal criminal surveillance law.

"I think it's a stretch" of previous federal legal interpretations, says Mr. Eckenwiler, who hasn't seen the secret ruling. If a federal attorney "served a grand-jury subpoena for such a broad class of records in a criminal investigation, he or she would be laughed out of court."

Two senators on the Intelligence Committee, Ron Wyden (D., Ore.) and Mark Udall (D., Colo.), have argued repeatedly that there was a "secret interpretation" of the Patriot Act. The senators' offices tell the Journal that this new interpretation of the word "relevant" is what they meant. An official at FISC, the secret court, declined to comment. The NSA referred questions to the Justice Department, saying this provision of the Patriot Act addressed FBI authorities. The Justice Department didn't comment.

U.S. surveillance programs are under fresh scrutiny after Mr. Snowden, the former NSA contractor, among other things revealed a secret order from the surveillance court directing Verizon Business Services Inc. to turn over "comprehensive communications routing information" to the NSA. Mr. Snowden also revealed a classified draft of a 2009 NSA Inspector General report that provides further details on the phone program and a related one that gathered Internet data. Other large phone companies, including [AT&T Inc.](#) T +0.57% and [Sprint Nextel Corp.](#), S -1.26% receive similar orders every three months, former officials say.



Former Sen. Russ Feingold failed in his bid to use stricter wording.

Under the Patriot Act, the Federal Bureau of Investigation can require businesses to hand over "tangible things," including "records," as long as the FBI shows it is reasonable to believe the things are "relevant to an authorized investigation" into international terrorism or foreign intelligence activities.

The history of the word "relevant" is key to understanding that passage. The

Supreme Court in 1991 said things are "relevant" if there is a "reasonable possibility" that they will produce information related to the subject of the investigation. In criminal cases, courts previously have found that very large sets of information didn't meet the relevance standard because significant portions—innocent people's information—wouldn't be pertinent.

But the Foreign Intelligence Surveillance Court, FISC, has developed separate precedents, centered on the idea that investigations to prevent national-security threats are different from ordinary criminal cases. The court's rulings on such matters are classified and almost impossible to challenge because of the secret nature of the proceedings. According to the court, the special nature of national-security and terrorism-prevention cases means "relevant" can have a broader meaning for those investigations, say people familiar with the rulings.

The use of computers to look for links in massive data sets also means information previously not considered relevant could today, in fact, be important in some broad investigations, says Paul Rosenzweig, a former Deputy Assistant Secretary for Policy in the Department of Homeland Security in the administration of President George W. Bush.

"Large databases are effective" for this type of analysis "only to the extent they are actually comprehensive," says Mr.

Boss Is Building a New Empire



\$1 A WEEK FOR 12 WEEKS [SUBSCRIBE NOW](#)

Don't Miss

[?]



Beer Can Boats Stay Afloat



Opinion: Why Men are Boycotting Marriage



How Millennials Are Rewriting the Rules of Adulthood

More in US

- [Pilot Error Eyed in Crash](#)
- [Secret Court Ruling Expanded Spy Powers](#)
- [Derailment Fuels Crude-by-Rail Concerns](#)
- [China Mourns Student Deaths](#)
- [Teresa Heinz Kerry's Condition Upgraded](#)

Popular Now

What's This?

Opinion: ObamaCare's 'Liar' Subsidies



Harsh Words From Mayor's Daughter



Pilot Error Eyed in Crash



4 Secret Ruling Expanded Spy Powers



A Simple Portfolio of Three Funds



[Show 5 More](#)



Enlarge Image
Agence France-Presse/Getty Images
James Clapper, Director of National Intelligence, has defended the collection of large databases.

Rosenzweig, founder of homeland-security consultant Red Branch Consulting PLLC.

This explanation echoes recent statements by the Obama administration. "More narrow collection would limit our ability to screen for and identify terrorism-related communications," said James Clapper, Director of National Intelligence, in a statement June 6.

People familiar with the system that uses phone records in investigations say that the court's novel legal theories allow the system to include bulk phone records, as long as there are privacy safeguards to limit searches. NSA analysts may query the database only "when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization," according to Mr. Clapper.

The NSA database includes data about people's phone calls—numbers dialed, how long a call lasted—but not the actual conversations. According to Supreme Court rulings, a phone call's content is covered by the Constitution's Fourth Amendment, which restricts unreasonable searches, but the other types of data aren't.

The idea that large databases of American activity were needed to prevent terrorism gained steam following the terror attacks of Sept. 11, 2001. Soon after, the Bush administration began several expanded surveillance efforts.

Amid controversy over the programs starting in 2004, the administration agreed to move domestic Internet data collection under the authority of FISC orders, according to the Inspector General's report revealed by Mr. Snowden. (That Internet data collection program ended in 2011, the NSA has said.) By 2006, the administration looked to move the phone-records program under the court as well, according to the report.



Enlarge Image
Associated Press
Sen. Ron Wyden has said there was a 'secret interpretation' of the Patriot Act.

In 2005 and early 2006, some lawmakers tried to tighten the Patriot Act when it came up for reauthorization. At that time, the part of the law being used to get phone records required investigators simply to state that records were sought for an authorized investigation into terrorism or foreign intelligence—a lower standard than "relevant." Congress added the word "relevant" to the law, but senators who wanted even stricter standards—which

would have ended the ability to collect bulk phone records—failed.

Former Sen. Jon Kyl spoke on the floor of the Senate in favor of the "relevance" standard. "We all know the term 'relevance.' It is a term that every court uses," he said in 2006. "The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation," he said.

But a few people cautioned that "relevant" could be defined to the point of irrelevance. "Relevance is a very broad standard that could arguably justify the collection of all kinds of information about law-abiding Americans," former Sen. Russ Feingold said on the Senate floor in February 2006. He argued for stricter wording, and failed.

Raspberry Pill Melts Fat?

Celebrity Doctor Exposes One Weird Fruit That Melts Your Fat Fast...
PureRaspberryKetone.com

(1200%) Stock?

Will This \$0.50 Stock Hit \$6.00? Will \$10,000 Turns Into \$120,000?
TheLifeWiki.com

Arrest Records Now Online

1) Enter Name and State. 2) Access Anyone's Public Records Instantly.
instantcheckmate.com

Content from our Sponsors [?]



SALARY.COM
8 College Degrees That Don't Pay Off



ANCESTRY.COM
What Vanessa Williams Learned About Her Family Tree from a DNA Test



ABOUT.COM
What NOT to Do on a Caribbean Vacation

President Bush signed the Patriot Act reauthorization in March 2006. And the NSA and Justice Department set about persuading the secret court, FISC, that the law allowed them to obtain bulk phone records.

The Bush administration didn't see the argument as a difficult one to make. According to the draft Inspector General's report revealed by Mr. Snowden, the administration had won court approval of the Internet data program two years before, something that made it easier to answer the court's questions. Of the requirement to show "relevance," a former official familiar with the discussions at the time says: "Usually, it's a pretty generous standard."

The court did limit the number of people who could access the data, and it required "more stringent oversight" by the Justice Department, according to the Inspector General's report. But in May 2006, the secret court agreed that, even with the addition of the word "relevant," bulk phone records could also be collected under the law.

The legal interpretations required to make this change were "aggressive," says Timothy Edgar, a former top privacy lawyer at the Office of the Director of National Intelligence and the National Security Council in the Bush and Obama administrations. Still, considering that the program previously had less congressional or court oversight, many lawmakers saw this as a step forward, he says.

"It wasn't seen that we're pushing the boundaries of surveillance law here," Mr. Edgar says. "It was the very opposite. You're starting from a huge amount of unilateral surveillance and putting it on a much sounder legal basis."

Some lawmakers now disagree. "The government must request specific records relevant to its investigation," Rep. Jim Sensenbrenner (R., Wis.), one of the authors of the Patriot Act, says. "To argue otherwise renders the provision meaningless," he says. "It's like scooping up the entire ocean to guarantee you catch a fish."

Given the traditional legal definition of relevant, Mr. Edgar says, it is "a fair point" to say that someone reading the law might believe it refers to "individualized requests" or "requests in small batches, rather than in bulk database form." From that standpoint, he says, the reinterpretation of relevant amounts to "secret law."

Still, he says, Congress repeatedly had the option to prohibit in legislation the bulk collection of records, and it didn't.

Defenders of using the Patriot Act this way make similar arguments. In a statement last month, the chair and ranking minority member on the Senate Intelligence Committee said that both the House and Senate Intelligence and Judiciary committees have "been briefed extensively" on this.

Mr. Edgar added, however, that Congress couldn't fully debate the issue because the program wasn't public.

Write to Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com and Siobhan Gorman at siobhan.gorman@wsj.com

JOIN THE DISCUSSION
229 Comments, add yours

MORE IN
US »

Email Print Order Reprints

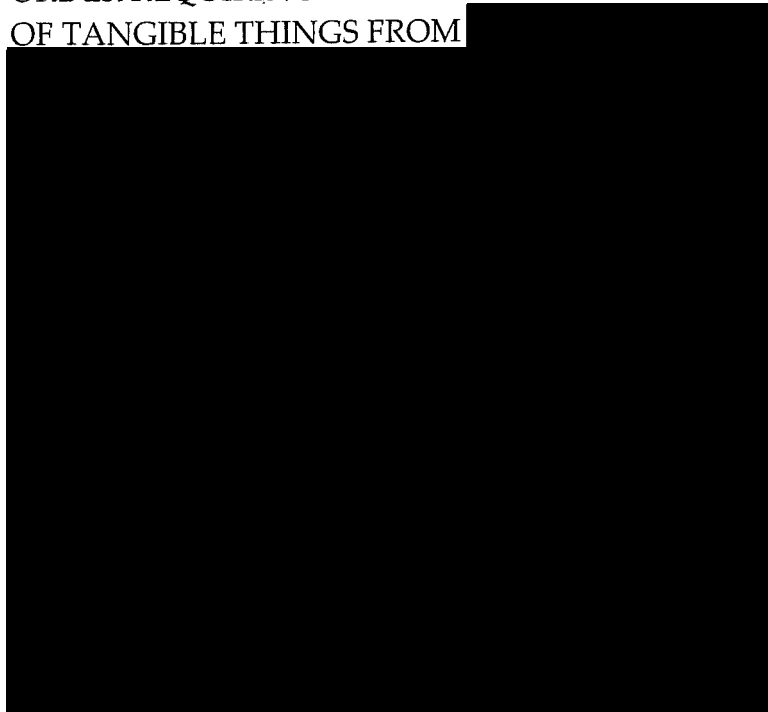
THE NEW PORTFOLIO TOOL ON WSJ.COM:
THE ULTIMATE INVESTMENT TRACKER
AVAILABLE EXCLUSIVELY FOR SUBSCRIBERS
LEARN MORE
provided by LikeAssets

EXHIBIT D

~~TOP SECRET//COMINT//NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR

11-07

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//COMINT//NOFORN~~

Derived from: Pleadings in the above-captioned docket
Declassify on: 21 January 2036

~~TOP SECRET//COMINT//NOFORN~~

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 10-70 and its predecessors. [50 U.S.C. § 1861(c)(1)]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"¹ created by [REDACTED]

B. The Custodian of Records of [REDACTED]

[REDACTED]
[REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

¹ For purposes of this Order "telephony metadata" includes comprehensive communications routing information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or “telephony metadata” created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED]

[REDACTED]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court’s orders in the above-captioned docket and its predecessors (“BR metadata”) for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA’s control.² The BR metadata shall carry unique markings such

² The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA will ensure that any access

~~TOP SECRET//COMINT//NOFORN~~

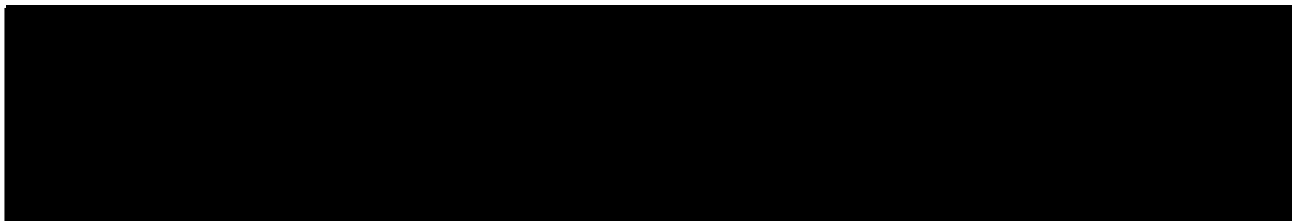
~~TOP SECRET//COMINT//NOFORN~~

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.³

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using identifiers⁴ that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes, but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may query the BR metadata with a non-RAS-approved identifier to determine whether that identifier is a high volume identifier. If so, the technician may share the results of that query, *i.e.*, the identifier and the fact that it is a

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

³ The Court understands that certain technical personnel, specifically the personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.



~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

high volume identifier, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that query for intelligence analysis purposes.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata using identifiers approved as "seeds" pursuant to the RAS approval process described below, as described in the [REDACTED] Declaration at paragraph 17. NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only an identifier that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.

(i) Except as provided in subparagraph (ii) below, all identifiers to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the identifier to be queried is associated with [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

provided, however, that NSA's OGC shall first determine that any identifier reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [REDACTED] [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution.⁷

(ii) Identifiers that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by agents of [REDACTED] [REDACTED] including those used by U.S. persons, may be

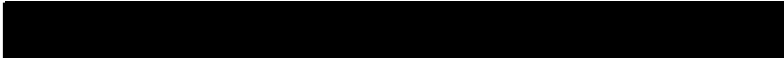
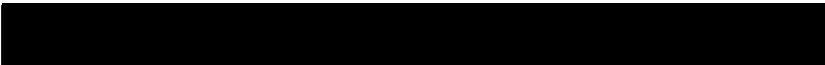
⁷ The Court understands that from time to time the information available to designated approving officials will indicate that an identifier is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the identifier is or was associated with a Foreign Power will be specified so that analysts conducting queries using that identifier can properly minimize information that may be returned within query results that fall outside of that timeframe.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official.

The preceding sentence shall not apply to identifiers under surveillance pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that an identifier is associated with  shall be effective for:  one hundred eighty days for U.S. identifiers and for any identifiers believed to be used by a U.S. person; one year for all other identifiers.⁸

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

D. Results derived from any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.⁹ NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) to any results from queries of the BR metadata disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (*i.e.*, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operation Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.¹⁰

⁹ In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

¹⁰ In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Notwithstanding the above requirements, NSA may share results derived from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the

modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.¹¹ OGC shall provide NSD/DoJ with copies of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of a sample of the call detail records obtained to ensure

¹¹ The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the information derived therefrom.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for identifiers used to query the BR metadata.

(vii) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of the queries made since the last report and NSA's application of the RAS standard. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, information derived from the BR metadata with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

-- Remainder of page intentionally left blank. --

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

This authorization regarding [REDACTED]

and unknown persons in the United States and abroad affiliated with [REDACTED]

[REDACTED]

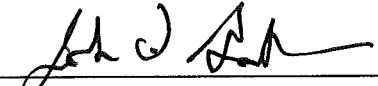
[REDACTED] and unknown persons in the United States and abroad affiliated with

[REDACTED] expires on the 15th day

of April, 2011, at 5:00 p.m., Eastern Time.

01-20-2011 P02:39

Signed _____ Eastern Time
Date Time



JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

I, [REDACTED] Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

EXHIBIT E



Office of the Deputy Attorney General
Washington, D.C. 20530

January 27, 2014

Sent via Email

Colin Stretch, Esquire
Vice President and General Counsel
Facebook Corporate Office
1601 Willow Road
Menlo Park, CA 94025

Kent Walker, Esquire
Senior Vice President and General Counsel
Google Corporate Office Headquarters
1600 Amphitheater Parkway
Mountain View, CA 94043

Erika Rottenberg, Esquire
Vice President, General Counsel/Secretary
LinkedIn Corporation
2029 Stierlin Court
Mountain View, CA 94043

Brad Smith, Esquire
Executive Vice President and General Counsel
Microsoft Corporate Office Headquarters
One Microsoft Way
Redmond, WA 98052-7329

Ronald Bell, Esquire
General Counsel
Yahoo Inc. Corporate Office and Headquarters
701 First Avenue
Sunnyvale, CA 94089

Dear General Counsels:

Pursuant to my discussions with you over the last month, this letter memorializes the new and additional ways in which the government will permit your company to report data concerning requests for customer information. We are sending this in connection with the Notice we filed with the Foreign Intelligence Surveillance Court today.

In the summer of 2013, the government agreed that providers could report in aggregate the total number of all requests received for customer data, including all criminal process, NSLs,

Letter to Colin Stretch, Kent Walker, Erika Rottenberg, Brad Smith and Ronald Bell

Page 2

and FISA orders, and the total number of accounts targeted by those requests, in bands of 1000. In the alternative, the provider could separately report precise numbers of criminal process received and number of accounts affected thereby, as well as the number of NSLs received and the number of accounts affected thereby in bands of 1000. Under this latter option, however, a provider could not include in its reporting any data about FISA process received.

The government is now providing two alternative ways in which companies may inform their customers about requests for data. Consistent with the President's direction in his speech on January 17, 2014, these new reporting methods enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

Option One.

A provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.
2. The number of NSLs received, reported in bands of 1000 starting with 0-999.
3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999.
4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.
5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.
6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.¹
7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.

A provider may publish the FISA and NSL numbers every six months. For FISA information, there will be a six-month delay between the publication date and the period covered

¹ As the Director of National Intelligence stated on November 18, 2013, the Government several years ago discontinued a program under which it collected bulk internet metadata, and no longer issues FISA orders for such information in bulk. See <http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence>. With regard to the bulk collection of telephone metadata, the President has ordered a transition that will end the Section 215 bulk metadata program as it currently exists and has requested recommendations about how the program should be restructured. The result of that transition will determine the manner in which data about any continued collection of that kind is most appropriately reported.

Letter to Colin Stretch, Kent Walker, Erika Rottenberg, Brad Smith and Ronald Bell
Page 3

by the report. For example, a report published on July 1, 2015, will reflect the FISA data for the period ending December 31, 2014.

In addition, there will be a delay of two years for data relating to the first order that is served on a company for a platform, product, or service (whether developed or acquired) for which the company has not previously received such an order, and that is designated by the government as a "New Capability Order" because disclosing it would reveal that the platform, product, or service is subject to previously undisclosed collection through FISA orders. For example, a report published on July 1, 2015, will not reflect data relating to any New Capability Order received during the period ending December 31, 2014. Such data will be reflected in a report published on January 1, 2017. After data about a New Capability Order has been published, that type of order will no longer be considered a New Capability Order, and the ordinary six-month delay will apply.

The two-year delay described above does not apply to a FISA order directed at an enhancement to or iteration of an existing, already publicly available platform, product, or service when the company has received previously disclosed FISA orders of the same type for that platform, product, or service.

A provider may include in its transparency report general qualifying language regarding the existence of this additional delay mechanism to ensure the accuracy of its reported data, to the effect that the transparency report may or may not include orders subject to such additional delay (but without specifically confirming or denying that it has received such new capability orders).

Option Two.

In the alternative, a provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.
2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.
3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

* * *

I have appreciated the opportunity to discuss these issues with you, and I am grateful for the time, effort, and input of your companies in reaching a result that we believe strikes an appropriate balance between the competing interests of protecting national security and furthering transparency. We look forward to continuing to discuss with you ways in which the

Letter to Colin Stretch, Kent Walker, Erika Rottenberg, Brad Smith and Ronald Bell
Page 4

government and industry can similarly find common ground on other issues raised by the surveillance debates of recent months.

Sincerely,

A handwritten signature in black ink, appearing to read "James M. Cole". The signature is fluid and cursive, with a long horizontal stroke at the beginning and a smaller, more compact signature to the right.

James M. Cole
Deputy Attorney General

EXHIBIT F

The Washington Post

[Back to previous page](#)

Tech executives to Obama: NSA spying revelations are hurting business

**By [Cecilia Kang](#) and [Ellen Nakashima](#), Published:
December 17**

Leaders of the nation's biggest technology firms warned President Obama during a lengthy meeting at the White House on Tuesday that [National Security Agency spying programs](#) are damaging their reputations and could harm the broader economy.

[Cisco Systems](#) has said it is seeing customers, especially overseas, back away from American-branded technology after documents revealed that the NSA enlisted tech firms and secretly tapped into their data hubs around the world as the agency pursued terrorism suspects. Companies such as [IBM](#), [AT&T](#) and [Verizon Communications](#) are facing angry shareholders, some of whom have filed lawsuits demanding that the companies disclose their participation in NSA intelligence programs.

The companies also pressed the need for transparency and for limits on surveillance to restore the credibility of the U.S. government. They wanted an explanation of what the NSA was doing overseas to collect their data and to be able to talk about it, said industry and U.S. officials briefed on the meeting who spoke on the condition of anonymity to discuss it freely.

"Most companies" in the room pressed this point, "and they did so loudly," said one U.S. official.

Obama said that he heard their message and that the White House would consider the group's views as it completed a review of NSA surveillance programs.

Silicon Valley has been a critical driver of the economic recovery and has long represented the face of American ingenuity around the world. Many of these companies say they are still trying to assess the damage caused by [Edward Snowden's](#) leak of NSA documents showing their work with intelligence officials.

But some shareholders say Silicon Valley has been slow to recognize the reputational crisis that is developing around the world for these companies. "Verizon and AT&T are not managing this crisis effectively," said Jonas Kron, director of shareholder advocacy at Trillium, an investment advisory firm. "Now is the time for these companies to demonstrate that they will protect user privacy."

The morning meeting at the White House, held in the Roosevelt Room, took on added import given a federal judge's ruling Monday that [the NSA's counterterrorism program to collect Americans' phone records appears to be unconstitutional](#). That, along with the outcry from Silicon Valley and civil liberties advocates, some of whom belong to Obama's party, is increasing pressure on the administration to curb NSA surveillance efforts.

The gathering was scheduled for two hours but went well over the allotted time, with the majority of the discussion focused on the companies' demands for changes to NSA spying programs, according to tech industry officials.

Several of the executives came to the meeting particularly angered over a [Washington Post report](#) in late October that revealed the NSA and its British counterpart, Government Communications Headquarters, or GCHQ, were gaining access to the data connections that link [Google](#) and [Yahoo](#) servers around the world, industry officials said.

Their message was to say: "What the hell are you doing? Are you really hacking into the infrastructure of American companies

overseas? The same American companies that cooperate with your lawful orders and spend a lot of money to comply with them to facilitate your intelligence collection?" said one industry official familiar with the companies' views.

The NSA has stressed that its overseas collection is carried out lawfully, under executive authority. Any data on Americans are handled according to rules that protect their privacy, including the requirement to obtain a warrant to target an American's communications, officials say.

In the meeting, the executives reiterated a list of demands that had been sent to the White House in a letter last week calling on the administration to cease bulk data collection of e-mails, online address books and other personal information; to impose limits on how easily the NSA can obtain court orders for Internet data; and to allow the companies to be more transparent about government intelligence requests.

Several participants acknowledged that the White House had to balance the companies' business concerns against national security considerations.

Senior administration officials described the meeting with the 15 executives as "constructive, not at all contentious."

"This was an opportunity for the President to hear from CEOs directly as we near completion of our review of signals intelligence programs, building on the feedback we've received from the private sector in recent weeks and months," the White House said in a statement.

One participant suggested the president pardon Snowden. Obama said he could not do so, said one industry official. White House officials have said that Snowden is accused of leaking classified information and faces felony charges in the United States, and that he should be returned as soon as possible to the United States, "where he will be accorded full due process and protections."

Senior executives from AT&T, Yahoo, Apple, Netflix, Twitter, Google, Microsoft and Facebook were among those in attendance.

"We appreciated the opportunity to share directly with the President our principles on government surveillance that we released last week and we urged him to move aggressively on reform," the technology firms said in a joint statement after the meeting.

Many of these firms have played a key role in boosting Obama's political fortunes. Tech companies pumped nearly \$7.8 million into his campaign in the last cycle, according to the nonpartisan Center for Responsive Politics.

Some of the top officials meeting with the president Tuesday served as bundlers for his 2012 bid. Yahoo's chief executive, Marissa Mayer, raised between \$100,000 and \$200,000, according to the center, and Shervin Pishevar, co-founder of the Sherpa technology investment fund, raised more than \$500,000. Mark Pincus, Zynga's chief product officer and chairman, gave \$1 million to Priorities Action USA, the super PAC that supported Obama.

Still, some of these executives, as well as their shareholders, are fretting about the bottom-line impact of the NSA intelligence programs.

In Cisco's earnings report last month, executives explained that disappointing sales in emerging markets were partly tied to the NSA leaks, which may have "caused a number of customers to pause and reevaluate," Cisco's head of sales, Robert Lloyd, said at the time.

Last week, IBM shareholders sued the company in a New York federal court, saying that it harmed investors with its secret participation in NSA programs.

"IBM's association with the NSA presented a material risk to the company's sales and, in particular . . . sales in China that were of critical importance to investors," the Louisiana Sheriffs' Pension and Relief Fund said in its lawsuit. "Despite that knowledge . . . IBM misrepresented to investors that it was a market leader in the Asia-Pacific region and that IBM expected solid improvement in the sales of its hardware division."

Last month, shareholders of Verizon and AT&T demanded that the companies disclose their participation in NSA intelligence programs.

The \$160.7 billion New York State Common Retirement Fund filed a resolution with AT&T's board to make public its participation in government intelligence programs. The pension fund argued that customers can too easily switch to another wireless carrier amid concerns that AT&T is sharing telephone data and other information with the government.

The meeting at the White House was the second time top Silicon Valley and telecommunications leaders have convened with Obama since Snowden began to release portions of a trove of top-secret documents detailing NSA spying programs.

Obama tried to keep the tenor friendly, even cracking jokes, an industry official said.

At one point, he asked Netflix chief executive Reed Hastings if he brought advanced copies of the second season of "House of Cards," a satire-drama of Washington politics, according to a pool report of the meeting.

Hastings laughed and invited Obama to do a cameo appearance on the show. Obama said of the ruthless lead character, a congressman played by Kevin Spacey, "This guy's getting a lot of stuff done."

"I wish things were that ruthlessly efficient," Obama said, to laughter from all the tech executives.

Juliet Eilperin and Matea Gold contributed to this report.

Related stories: The Switch: Is Edward Snowden seeking the spotlight? New ruling threatens the legal foundation of the NSA's phone records program

Sponsored Links

Visa® Black Card™

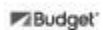
The World Awaits®. Apply Now to Get The New Stainless Steel Card Today!
BlackCard.com



What is Your Flood Risk?

Protect your home from floods. Get your flood risk profile today.
www.floodsmart.gov

Budget.com: Official Site



Rent A Car With Budget & Get Our Signature where2 GPS. Rent Today!
Budget.com/GPS

[Buy a link here](#)

© The Washington Post Company

EXHIBIT G

The Washington Post

[Back to previous page](#)

Tech industry: Obama's NSA reforms 'insufficient'

By Associated Press, Published: January 18

SAN FRANCISCO — Technology companies and industry groups took President Barack Obama's speech on U.S. surveillance as a step in the right direction, but chided him for not embracing more dramatic reforms to protect people's privacy and the economic interests of American companies that generate most of their revenue overseas.

"The president's speech was empathetic, balanced and thoughtful, but insufficient to meet the real needs of our globally connected world and a free Internet," said Ed Black, president of the Computer & Communications Industry Association, a group that represents Google, Microsoft, Facebook and other technology companies upset about the NSA's broad surveillance of online communications.

On Friday, the president called for ending the government's control of phone data from hundreds of millions of Americans and ordered intelligence agencies to get a court's permission before accessing such records. He also issued a directive that intelligence-gathering can't be employed to suppress criticism of the United States or provide a competitive advantage to U.S. companies.

In addition, the president directed Attorney General Eric Holder and Director of National Intelligence James Clapper to consider whether new privacy safeguards could be added to online data gathering. Although those activities are only meant to target people outside the U.S. as part of national security investigations, information on Americans sometimes gets swept up in the collection.

Eight of the world's best-known technology companies underscored their common interest in curbing the NSA by releasing a joint, measured critique of Obama's proposal. They applauded the commitment to more transparency and more privacy protections for non-U.S. citizens, but also stressed that the president didn't address all their concerns.

"Additional steps are needed on other important issues, so we'll continue to work with the administration and Congress to keep the momentum going and advocate for reforms consistent with the principles we outlined in December," said the statement from Google, Apple, Yahoo, Microsoft, Facebook, Twitter, LinkedIn and AOL.

In his speech, Obama also directed Holder and Clapper to look into new restrictions on the length of time the U.S. can hold data collected overseas and the extent to which that data is used. He added that the U.S. won't spy on regular people who don't threaten national security.

But nothing he said is likely to diminish the potential losses facing the U.S. technology industry, said Daniel Castro, a senior

analyst for the Information Technology and Innovation Foundation, a Washington D.C. think tank.

The ITIF estimates that the doubts raised by the NSA spying could cost U.S. companies as much as \$35 billion over the next three years.

In the aftermath of recent NSA leaks, the companies set aside their competitive differences to come together and urge Obama to curtail the NSA's online snooping and lift restrictions that prevent companies from publicly disclosing specifics about how frequently they are asked to turn over their users' personal information in the name of national security.

Obama did agree to at least one major concession to the technology industry by pledging "to make public more information than ever before about the orders they have received to provide data to the government." The companies are hoping greater transparency will show that the U.S. government has only been demanding information about a very small fraction of their vast audiences.

But the promise of more disclosure didn't satisfy two different groups focused on online privacy and other digital rights.

"Far more needs to be done to restore the faith of the American people and repair the damage done globally to the U.S. reputation as a defender of human rights on the Internet," said Greg Nojeim, senior counsel at the Center for Democracy & Technology.

Cindy Cohn, legal director for the Electronic Frontier Foundation believes there's still a long way to go. "Now it's up to the courts, Congress, and the public to ensure that real reform happens, including stopping all bulk surveillance — not just telephone records collection," she said.

Recent revelations about how much information the U.S. government has been vacuuming off the Internet threaten to undercut the future profits of technology companies that depend on the trust of Web surfers and corporate customers.

U.S. Internet companies are worried that more people, especially those living outside the U.S., will use their products less frequently if they believe their personal data is being scooped up and stored by the U.S. government.

Less online traffic would result in fewer opportunities to sell the ads that bring in most of the revenue at companies such as Google, Facebook and Yahoo. There is also concern that foreigners will be reluctant to do business with a wide range of U.S. companies that sell online storage and software applications that require an Internet connection.

Obama's proposal made "progress on the privacy side, but it doesn't address the economic issues," Castro said. "I don't see anything in the speech that will prevent companies in other countries from using what the NSA is doing to gain a competitive advantage over the U.S. companies."

—

Ortutay reported from New York.

Copyright 2014 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Sponsored Links



Women: Low On Energy?

88 Year Old Yoga Teacher Shares Her Secret To Never Ending Energy
Health1st.com



What is Your Flood Risk?

Protect your home from floods. Get your flood risk profile today.
www.floodsmart.gov

Visa® Black Card™

Introducing the New Stainless Steel Visa Black Card. Apply Today!
BlackCard.com

[Buy a link here](#)

© The Washington Post Company

EXHIBIT H

The Washington Post

[Back to previous page](#)

Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic

By [Craig Timberg](#), [Barton Gellman](#) and [Ashkan Soltani](#), Published: November 26

Microsoft is moving toward a major new effort to encrypt its Internet traffic amid fears that the [National Security Agency](#) may have broken into its global communications links, said people familiar with the emerging plans.

Suspicions at Microsoft, while building for several months, sharpened in October when it was reported that the [NSA was intercepting traffic](#) inside the private networks of Google and Yahoo, two industry rivals with similar global infrastructures, said people with direct knowledge of the company's deliberations. They said top Microsoft executives are meeting this week to decide what encryption initiatives to deploy and how quickly.

Documents obtained from [former NSA contractor Edward Snowden](#) suggest — but do not prove — that the company is right to be concerned. [Two previously unreleased slides](#) that describe operations against Google and Yahoo include references to Microsoft's Hotmail and Windows Live Messenger services. [A separate NSA e-mail](#) mentions Microsoft Passport, a Web-based service formerly offered by [Microsoft](#), as a possible target of that same surveillance project, called MUSCULAR, which was first disclosed by The Washington Post last month.

Though Microsoft officials said they had no independent verification of the NSA targeting the company in this way, general counsel Brad Smith said Tuesday that it would be “very disturbing” and a possible constitutional breach if true.

Microsoft's move to expand encryption would allow it to join [Google](#), [Yahoo](#), [Facebook](#) and other major technology firms in hardening its defenses in response to news reports about once-secret NSA programs. The resulting new investments in encryption technology stand to complicate surveillance efforts — by governments, private companies and criminals — for years, experts say.

Though several legislative efforts are underway to curb the NSA's surveillance powers, the wholesale move by private companies to expand the use of encryption technology may prove to be the most tangible outcome of months of revelations based on documents that Snowden provided to The Post and Britain's Guardian newspaper. In another major shift, the companies also are explicitly building defenses against U.S. government surveillance programs in addition to combating hackers, criminals or foreign intelligence services.

“That's a pretty big change in the way these companies have operated,” said Matthew Green, a Johns Hopkins University cryptography expert. “And it's a big engineering effort.”

In response to questions about Microsoft, the NSA said in a statement Tuesday, “NSA's focus is on targeting the communications of valid foreign intelligence targets, not on collecting and exploiting a class of communications or services that would sweep up communications that are not of bona fide foreign intelligence interest to the U.S. government.”

A U.S. official, who was not authorized to discuss the matter publicly and spoke on the condition of anonymity, said Tuesday that collection can be done at various points and does not necessarily happen on a company's private fiber-optic links.

A [2009 e-mail](#) from a senior manager of the NSA's MUSCULAR project specifies that a targeting tool called “MONKEY

PUZZLE” is capable of searching only across certain listed “realms,” including Google, Yahoo and Microsoft’s Passport service. It is not clear what service a fourth listed realm, “emailAddr,” refers to. “NSA could send us whatever realms they like right now, but the targeting just won’t go anywhere unless it’s of one of the above 4 realms,” the e-mail said.

The tech industry’s response to revelations about NSA surveillance has grown far more pointed in recent weeks as it has become clear that the government was gathering information not only through court-approved channels in the United States — overseen by the [Foreign Intelligence Surveillance Court](#) — but also through the massive data links overseas, where the NSA needs authority only from the president. That form of collection has been done surreptitiously by gaining access to fiber-optic connections on foreign soil.

Smith, the Microsoft general counsel, hinted at the extent of the company’s growing encryption effort at a shareholders meeting last week. “We’re focused on engineering improvements that will further strengthen security,” he said, “including strengthening security against snooping by governments.”

People familiar with the company’s planning, who spoke on the condition of anonymity to discuss matters not yet publicly announced, said that while officials do not have definitive proof that the NSA has targeted Microsoft’s communication links, they have been engaged in a series of high-level meetings to pursue encryption initiatives “across the full range of consumer and business services.” A cost estimate was not available; key decisions are due to be made at a meeting of top executives this week in Redmond, Wash., where Microsoft is headquartered.

When asked about the NSA documents mentioning surveillance of Microsoft services, Smith issued a sharply worded statement: “These allegations are very disturbing. If they are true these actions amount to hacking and seizure of private data and in our view are a breach of the protection guaranteed by the Fourth Amendment to the Constitution.”

That echoes a similar statement by Google’s general counsel, [David Drummond](#), who said last month that he was “outraged” by the report in The Post about the [NSA tapping into the links connecting the company’s network of data centers](#). Google in September announced an ambitious [new set of encryption initiatives](#), including among data centers around the world. Yahoo made a [similar announcement](#) last week.

Microsoft, Google and Yahoo also have joined other [major tech firms](#), including [Apple](#), Facebook and [AOL](#), in calling for limits to the NSA’s surveillance powers. Most major U.S. tech companies are struggling to cope with a global backlash over U.S. snooping into Internet services.

The documents provided by Snowden are not entirely clear on the way the NSA might gain access to Microsoft’s data, and it is possible that some or all of it happens on the public Internet as opposed to on the private data center links leased by the company. But several documents about MUSCULAR, the NSA project that collects communications from links between Google and Yahoo data centers, discuss targeting Microsoft online services. The company’s Hotmail e-mail service also is one of several from which the NSA has collected users’ online address books.

The impact of Microsoft’s move toward expanded encryption is hard to measure. And even as most major Internet services move to encrypt their communications, they typically are decoded — at least briefly — as they move between different companies’ systems, making them vulnerable.

Privacy activists long have criticized Microsoft as lagging behind some rivals, such as Google and [Twitter](#), in implementing encryption technology. A widely cited scorecard of privacy and security by tech companies, compiled by the Electronic Frontier Foundation in San Francisco, gives Microsoft a single check mark out of a possible five.

“Microsoft is not yet in a situation where we really call them praiseworthy,” said Peter Eckersley, director of technology projects at the foundation. “Microsoft has no excuse for not being a leader in encryption and security systems, and yet we often see them lagging behind the industry.”

Encryption, while not impervious to targeted surveillance, makes it much more difficult to read communications in bulk as they travel the Internet. The NSA devotes substantial resources to decoding encrypted traffic, but the work is more targeted and time consuming, sometimes involving hacking into individual computers of people using encryption technology.

Documents provided by Snowden, and first reported by the Guardian, show that Microsoft worked with U.S. officials to help circumvent some forms of encryption on the company’s services. Microsoft has disputed the Guardian report and said it provides information to the government only when legally compelled to do so.

Soltani is an independent security researcher and consultant.