The Washington Post

FRIDAY, JUNE 7, 2013

U.S. mines Internet firms' data, documents show

Google, Facebook, Apple, Yahoo deny giving NSA direct access to servers

by Barton Gellman and Laura Poitras

The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post.

The program, code-named PRISM, has not been made public until now. It may be the first of its kind. The NSA prides itself on stealing secrets and breaking codes, and it is accustomed to corporate partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google or Facebook before, and it is unlikely that there are richer troves of valuable intelligence than the ones in Silicon Valley.

Equally unusual is the way the NSA extracts what it wants, according to the document: "Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple."

London's Guardian newspaper reported Friday that GCHQ, Britain's equivalent of the NSA, also has been secretly gathering intelligence from the same internet companies through an operation set up by the NSA.

According to documents obtained by The Guardian, PRISM would appear to allow GCHQ to circumvent the formal legal process required in Britain to seek personal material such as emails, photos and videos from an internet company based outside of the country.

PRISM was launched from the ashes of President George W. Bush's secret program of warrantless domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligence Surveillance Court forced the president to look for new authority.

Congress obliged with the Protect America Act in 2007 and the FISA Amendments Act of 2008, which immunized private companies that cooperated voluntarily with U.S. intelligence collection. PRISM recruited its first partner, Microsoft, and began six years of rapidly growing data collection beneath the surface of a roiling national debate on surveillance and privacy. Late last year, when critics in Congress sought changes in the FISA Amendments Act, the only lawmakers who knew about PRISM were bound by oaths of office to hold their tongues.

The court-approved program is focused on foreign communications traffic, which often flows through U.S. servers even when sent from one overseas location to another. Between 2004 and 2007, Bush administration lawyers persuaded federal FISA judges to issue surveillance orders in a fundamentally new form. Until then the government had to show probable cause that a particular "target" and "facility" were both connected to terrorism or espionage.

In four new orders, which remain classified, the court defined massive data sets as "facilities" and agreed to certify periodically that the government had reasonable procedures in place to minimize collection of "U.S. persons" data without a warrant.

In a statement issue late Thursday, Director of National Intelligence James R.

Clapper said "information collected under this program is among the most important and valuable foreign intelligence information we collect, and is used to protect our nation from a wide variety of threats. The unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans."

Clapper added that there were numerous inaccuracies in reports about PRISM by The Post and the Guardian newspaper, but he did not specify any.

Jameel Jaffer, deputy legal director of the American Civil Liberties Union, said: "I would just push back on the idea that the court has signed off on it, so why worry? This is a court that meets in secret, allows only the government to appear before it, and publishes almost none of its opinions. It has never been an effective check on government."

Several companies contacted by The Post said they had no knowledge of the program, did not allow direct government access to their servers and asserted that they responded only to targeted requests for information.

"We do not provide any government organization with direct access to Facebook servers," said Joe Sullivan, chief security officer for Facebook. "When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law."

"We have never heard of PRISM," said Steve Dowling, a spokesman for Apple. "We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order."

It is possible that the conflict between the PRISM slides and the company spokesmen is the result of imprecision on the part of the NSA author. In another classified report obtained by The Post, the arrangement is described as allowing "collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations," rather than directly to company servers.

Government officials and the document itself made clear that the NSA regarded the identities of its private partners as PRISM's most sensitive secret, fearing that the companies would withdraw from the program if exposed. "98 percent of PRISM production is based on Yahoo, Google and Microsoft; we need to make sure we don't harm these sources," the briefing's author wrote in his speaker's notes.

An internal presentation of 41 briefing slides on PRISM, dated April 2013 and intended for senior analysts in the NSA's Signals Intelligence Directorate, described the new tool as the most prolific contributor to the President's Daily Brief, which cited PRISM data in 1,477 items last year. According to the slides and other supporting materials obtained by The Post, "NSA reporting increasingly relies on PRISM" as its leading source of raw material, accounting for nearly 1 in 7 intelligence reports.

That is a remarkable figure in an agency that measures annual intake in the trillions of communications. It is all the more striking because the NSA, whose lawful mission is foreign intelligence, is reaching deep inside the machinery of American companies that host hundreds of millions of American-held accounts on American soil.

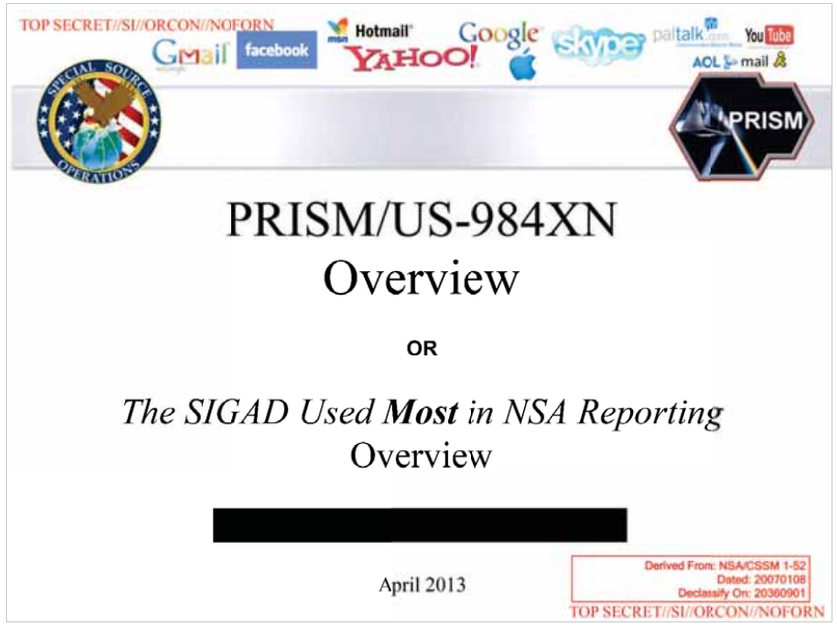
The technology companies, whose cooperation is essential to PRISM operations, include most of the dominant global players of Silicon Valley, according to the document. They are listed on a roster that bears their logos in order of entry into the program: "Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple." PalTalk, although much smaller, has hosted traffic of substantial intelligence interest during the Arab Spring and in the ongoing Syrian civil war.

Dropbox, the cloud storage and synchronization service, is described as "coming soon."

Sens. Ron Wyden (D-Ore.) and Mark Udall (D-Colo.), who had classified knowledge of the program as members of the Senate Intelligence Committee, were unable to speak of it when they warned in a Dec. 27, 2012, floor debate that the FISA Amendments Act had what both of them called a "back-door search loophole" for the content of innocent Americans who were swept up

The PRISM program: Slides show technique, types of data

Through a top-secret program authorized by federal judges working under the Foreign Intelligence Surveillance Act (FISA), the U.S. intelligence community can gain access to the servers of nine Internet companies for a wide range of digital data. Documents describing the previously undisclosed program, obtained by The Washington Post, show the breadth of U.S. electronic surveillance capabilities in the wake of a widely publicized controversy over warrantless wiretapping of U.S. domestic telephone communications in 2005. These slides, annotated by The Washington Post, represent a portion of the overall document, and certain portions are redacted.

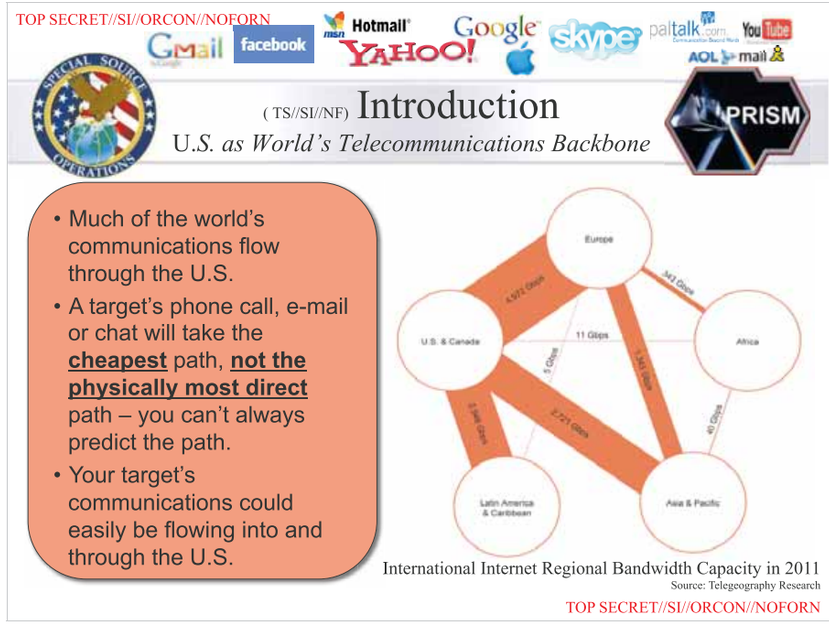


INTRODUCING THE PROGRAM
A slide briefing analysts at the National Security Agency about the program touts its effectiveness and features the logos of the companies involved.

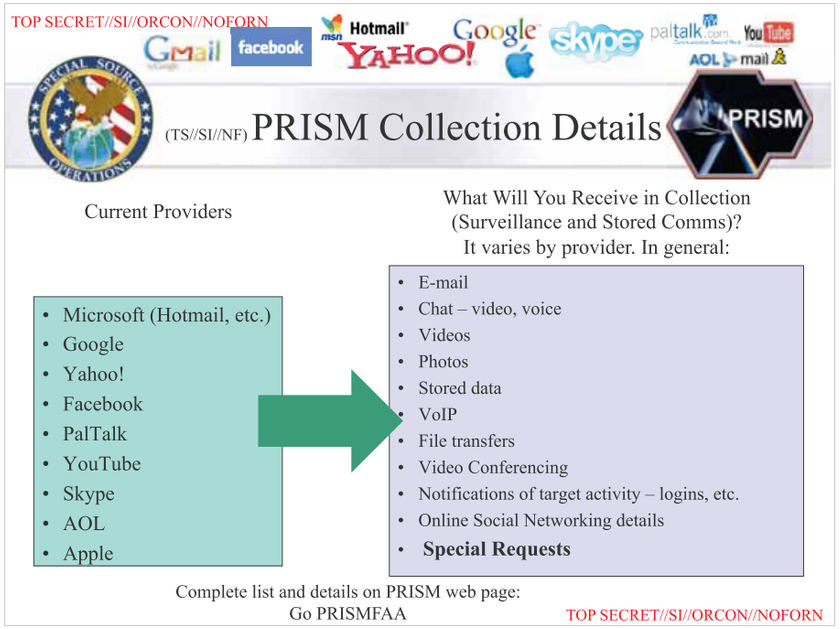
Upper right: The program is called PRISM, after the prisms used to split light, which is used to carry information on fiber-optic cables.

Lower right: This note indicates that the program is the number one source of raw intelligence used for NSA analytic reports.

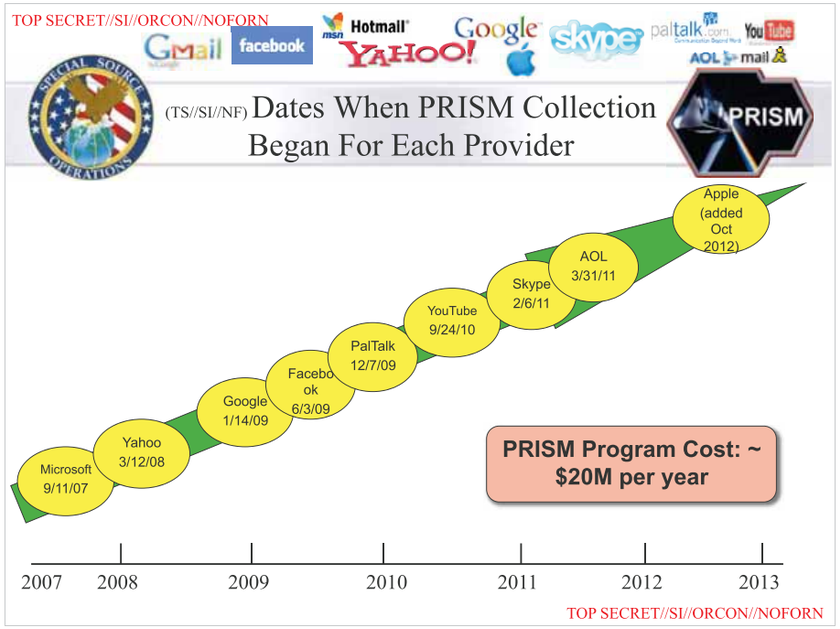
Upper left: The seal of Special Source Operations, the NSA term for alliances with trusted U.S. companies.



MONITORING A TARGET'S COMMUNICATION
This diagram shows how the bulk of the world's electronic communications moves through companies based in the United States.



PROVIDERS AND DATA
The PRISM program collects a wide range of data from the nine companies, although the details vary by provider.



PARTICIPATING PROVIDERS
This slide shows when each company joined the program, with Microsoft being the first, on Sept. 11, 2007, and Apple the most recent, in October 2012.

in a search for someone else.

"As it is written, there is nothing to prohibit the intelligence community from searching through a pile of communications, which may have been incidentally or accidentally been collected without a warrant, to deliberately search for the phone calls or e-mails of specific Americans," Udall said.

Wyden repeatedly asked the NSA to estimate the number of Americans whose communications had been incidentally collected, and the agency's director, Lt. Gen. Keith B. Alexander, insisted there was no way to find out. Eventually Inspector General I. Charles McCullough III wrote Wyden a letter stating that it would violate the privacy of Americans in NSA data banks to try to estimate their number.

Roots in the '70s

PRISM is an heir, in one sense, to a history of intelligence alliances with as many as 100 trusted U.S. companies since the 1970s. The NSA calls these Special Source Operations, and PRISM falls under that rubric.

The Silicon Valley operation works alongside a parallel program, code-named BLARNEY, that gathers up "metadata" — technical information about communications traffic and network devices — as it streams past choke points along the backbone of the Internet. BLARNEY's top-secret program summary, set down in the slides alongside a cartoon insignia of a shamrock and a leprechaun hat, describes it as "an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks."

But the PRISM program appears to more nearly resemble the most controversial of the warrantless surveillance orders issued by President George W. Bush after the al-Qaeda attacks of Sept. 11, 2001. Its history, in which President Obama presided over exponential growth in a program that candidate Obama criticized, shows how fundamentally surveillance law and practice have shifted away from individual suspicion in favor of systematic, mass collection techniques.

The Obama administration points to ongoing safeguards in the form of "extensive procedures, specifically approved by the court, to ensure that only non-U.S. persons outside the U.S. are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about U.S. persons."

And it is true that the PRISM program is not a dragnet, exactly. From inside a company's data stream the NSA is capable of pulling out anything it likes, but under current rules the agency does not try to collect it all.

Analysts who use the system from a Web portal at Fort Meade, Md., key in "selectors," or search terms, that are designed to produce at least 51 percent confidence in a target's "foreignness." That is not a very stringent test. Training materials obtained by The Post instruct new analysts to make quarterly reports of any accidental collection of U.S. content, but add that "it's nothing to worry about."

Even when the system works just as advertised, with no American singled out for targeting, the NSA routinely collects a great deal of American content. That is described as "incidental," and it is inherent in contact chaining, one of the basic tools of the trade. To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially. The same math explains the aphorism, from the John Guare play, that no one is more than "six degrees of separation" from any other person.

A 'directive'

In exchange for immunity from lawsuits, companies such as Yahoo and AOL are obliged to accept a "directive" from the attorney general and the director of national intelligence to open their servers to the FBI's Data Intercept Technology Unit, which handles liaison to U.S. companies from the NSA. In 2008, Congress gave the Justice Department authority for a secret order from the Foreign Surveillance Intelligence Court to compel a reluctant company

MANDEL NGAN/AGENCE FRANCE-PRESSE VIA GETTY IMAGES

President George W. Bush signs the FISA Amendments Act of 2008, which protected companies that cooperate with U.S. intelligence collection. In debate last year over proposed changes to the law, two senators expressed concerns about a "backdoor loophole" that could ensnare innocent Americans.

"to comply."

In practice, there is room for a company to maneuver, delay or resist. When a clandestine intelligence program meets a highly regulated industry, said a lawyer with experience in bridging the gaps, neither side wants to risk a public fight. The engineering problems are so immense, in systems of such complexity and frequent change, that the FBI and NSA would be hard pressed to build in back doors without active help from each company.

Apple demonstrated that resistance is possible when it held out for more than five years, for reasons unknown, after Microsoft became PRISM's first corporate partner in May 2007. Twitter, which has cultivated a reputation for aggressive defense of its users' privacy, is still conspicuous by its absence from the list of "private sector partners."

Google, like the other companies, denied that it permitted direct government access to its servers.

"Google cares deeply about the security of our users' data," a company spokesman said. "We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a 'back door' for the government to access private user data."

Microsoft also provided a statement: "We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don't participate in it."

Yahoo also issued a denial.

"Yahoo! takes users' privacy very seriously," the company said in a statement. "We do not provide the government with direct access to our servers, systems, or network."

Like market researchers, but with far more privileged access, collection managers in the NSA's Special Source Operations group, which oversees the PRISM program, are drawn to the wealth of information about their subjects in online accounts. For much the same reason, civil libertarians and some ordinary users may be trou-

bled by the menu available to analysts who hold the required clearances to "task" the PRISM system.

There has been "continued exponential growth in tasking to Facebook and Skype," according to the PRISM slides. With a few clicks and an affirmation that the subject is believed to be engaged in terrorism, espionage or nuclear proliferation, an analyst obtains full access to Facebook's "extensive search and surveillance capabilities against the variety of online social networking services."

According to a separate "User's Guide for PRISM Skype Collection," that service can be monitored for audio when one end of the call is a conventional telephone and for any combination of "audio, video, chat, and file transfers" when Skype users connect by computer alone. Google's offerings include Gmail, voice and video chat, Google Drive files, photo libraries, and live surveillance of search terms.

Firsthand experience with these systems, and horror at their capabilities, is what drove a career intelligence officer to provide PowerPoint slides about PRISM and supporting materials to The Washington Post in order to expose what he believes to be a gross intrusion on privacy. "They quite literally can watch your ideas form as you type," the officer said.

bart.gellman@washpost.com

Poitras is a documentary filmmaker and MacArthur Fellow. Julie Tate, Robert O'Harrow Jr., Cecilia Kang and Ellen Nakashima contributed to this report.