NSA slides explain the PRISM data-collection program

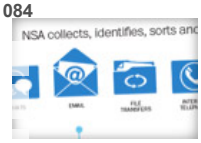
Published: June 6, 2013, Updated July 10, 2013

The top-secret PRISM program allows the U.S. intelligence community to gain access from nine Internet companies to a wide range of digital information, including e-mails and stored data, on foreign targets operating outside the United States. The program is court-approved but does not require individual warrants. Instead, it operates under a broader authorization from federal judges who oversee the use of the Foreign Intelligence Surveillance Act (FISA). Some documents describing the program were first released by The Washington Post on June 6. The newly released documents below give additional details about how the program operates, including the levels of review and supervisory control at the NSA and FBI. The documents also show how the program interacts with the Internet companies. These slides, annotated by The Post, represent a selection from the overall document, and certain portions are redacted. Read related article.

Related NSA graphics

1084

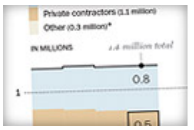
See the inner workings of the NSA's top secret spy program »



550,000 miles of undersea cables connect the world »

What is the Federal Intelligence Surveillance Court? »

Who holds top-secret security clearances? »



More

New slide published July 10

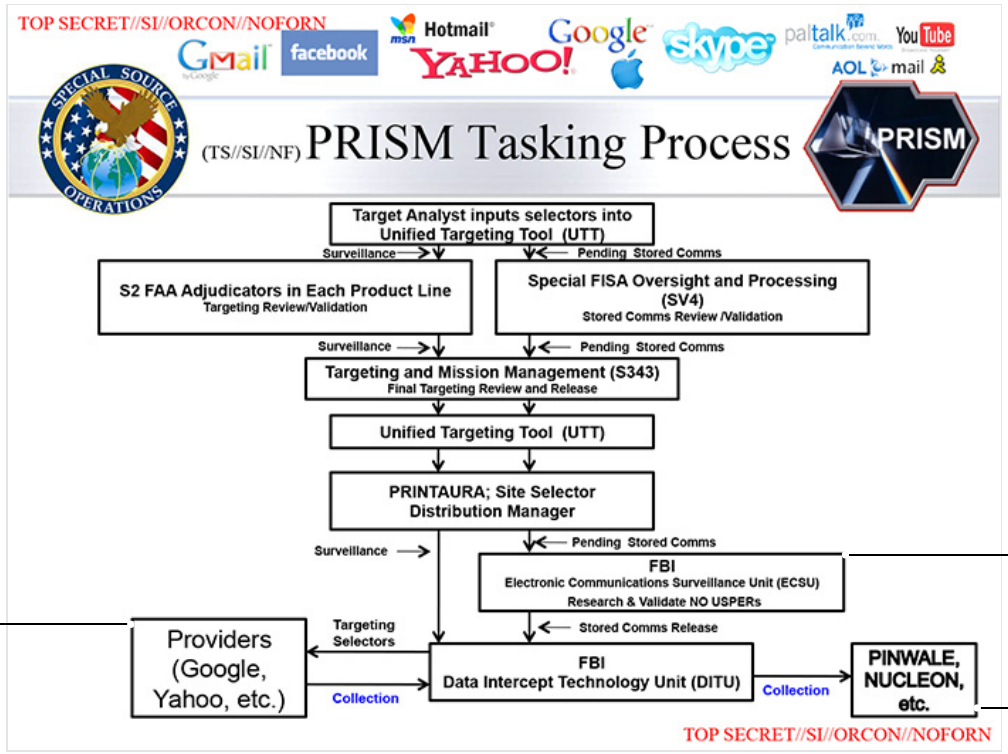
Upstream program

This slide shows PRISM as only one part of the NSA's system for electronic eavesdropping. The "Upstream" program collects from the fiber-optic cable networks that carry much of the world's Internet and phone data. The underlying map depicts the undersea cables that connect North America to the rest of the world.

Slides published June 29

Acquiring data from a new target

This slide describes what happens when an NSA analyst "tasks" the PRISM system for information about a new surveillance target. The request to add a new target is passed automatically to a supervisor who reviews the "selectors," or search terms. The supervisor must endorse the analyst's "reasonable belief," defined as 51 percent confidence, that the specified target is a foreign national who is overseas at the time of collection.



The FBI uses government equipment on private company property to retrieve matching information from **a participating company**, such as Microsoft or Yahoo and pass it without further review to the NSA.

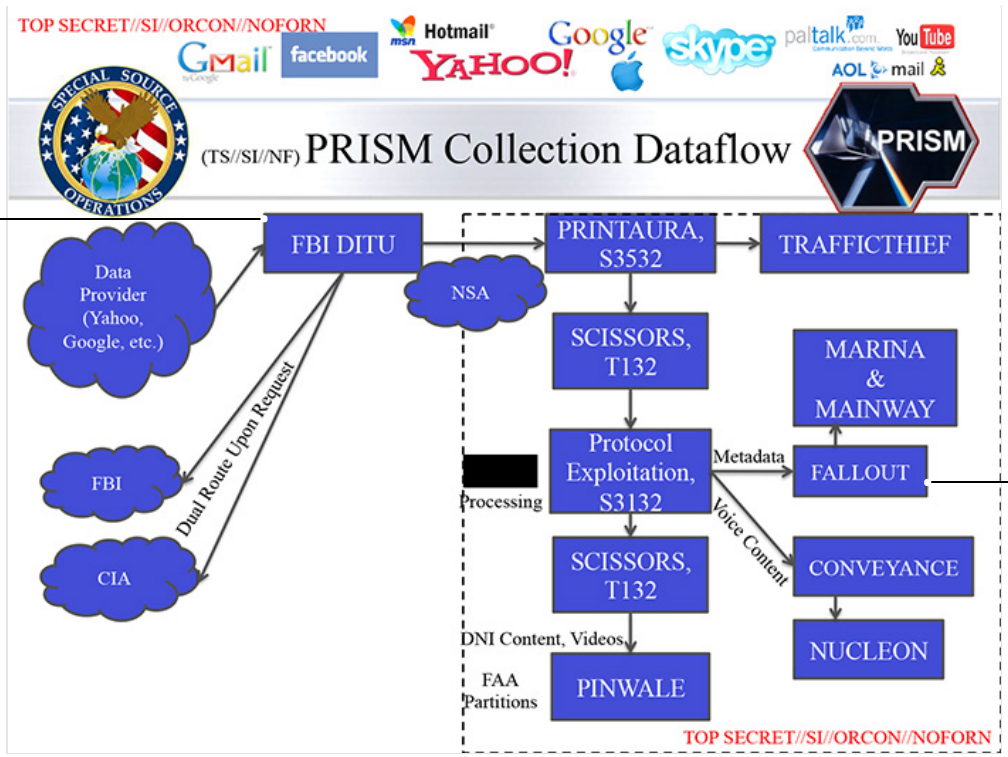
For stored communications, but not for live surveillance, the FBI consults its own databases to make sure the selectors do not match known Americans.

This is where data enters NSA systems, described more fully on the next slide.

The Foreign Intelligence Surveillance Court does not review any individual collection request.

Analyzing information collected from private companies

After communications information is acquired, the data are processed and analyzed by specialized systems that handle voice, text, video and "digital network information" that includes the locations and unique device signatures of targets.



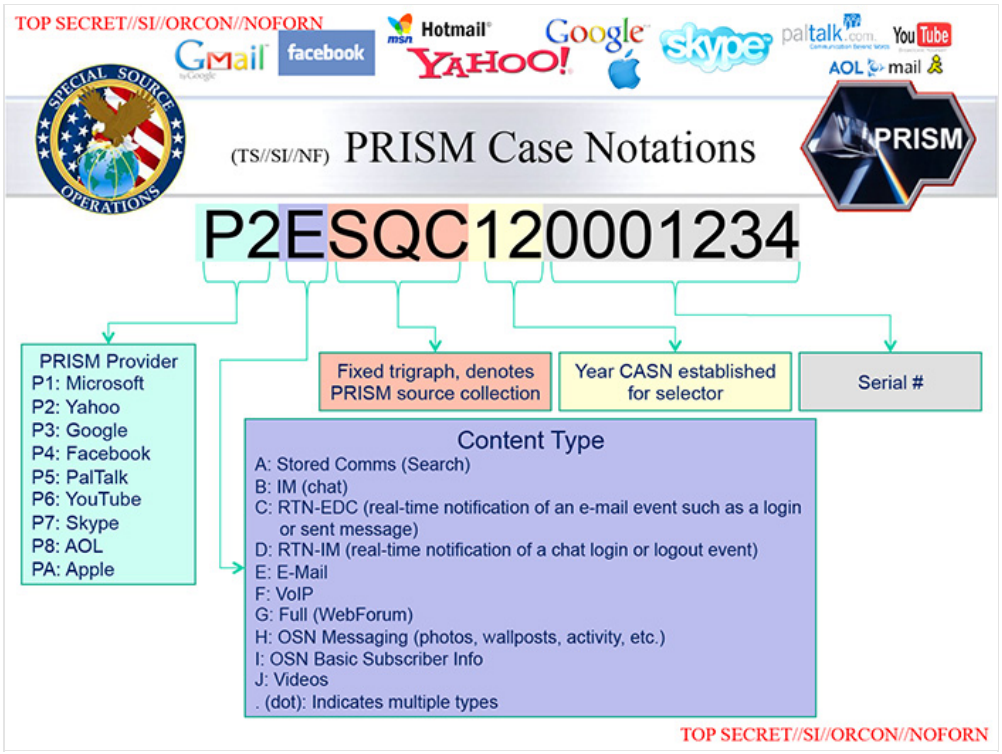
From the FBI's interception unit on the premises of private companies, the information is passed to one or more "customers" at the NSA, CIA or FBI.

PRINTAURA automates the traffic flow. **SCISSORS** and **Protocol Exploitation** sort data types for analysis in **NUCLEON** (voice), **PINWALE** (video), **MAINWAY** (call records) and **MARINA** (Internet records).

The systems identified as **FALLOUT** and **CONVEYANCE** appear to be a final layer of filtering to reduce the intake of information about Americans.

Each target is assigned a case notation

The PRISM case notation format reflects the availability, confirmed by The Post's reporting, of real-time surveillance as well as stored content.



Depending on the provider, the NSA may receive live notifications when a target logs on or sends an e-mail, or may monitor a voice, text or voice chat as it happens (noted on the first slide as "Surveillance").

Searching the PRISM database

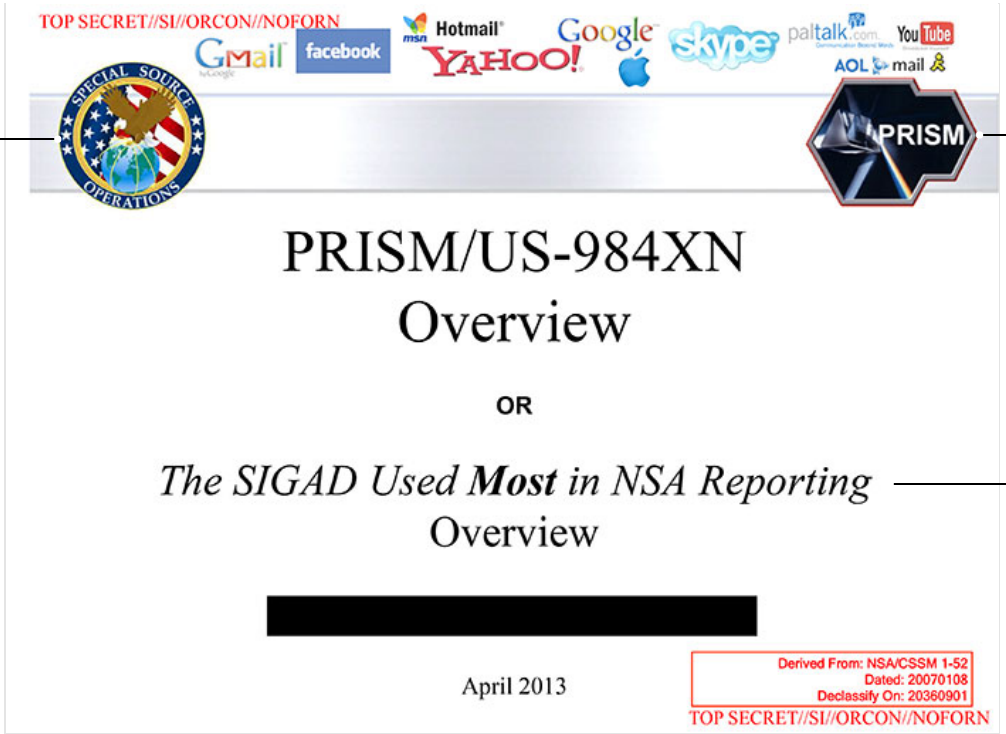
On April 5, according to this slide, there were 117,675 active surveillance targets in PRISM's counterterrorism database. The slide does not show how many other Internet users, and among them how many Americans, have their communications collected "incidentally" during surveillance of those targets.

Original slides published June 6

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.

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

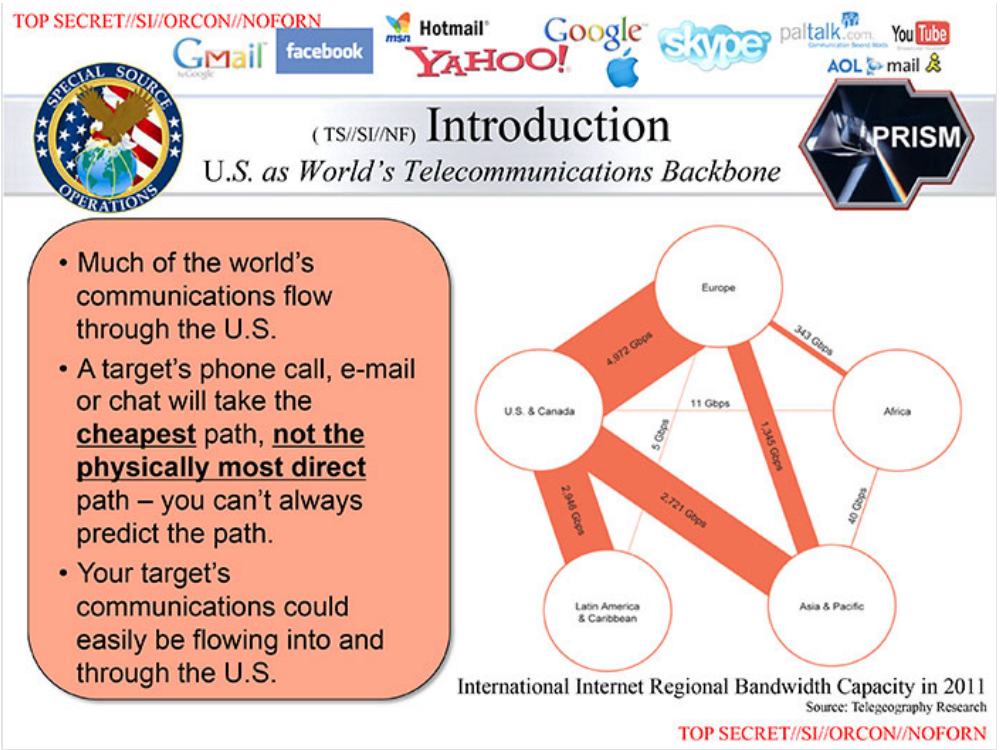


The program is called PRISM, after the prisms used to split light, which is used to carry information on fiber-optic cables.

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

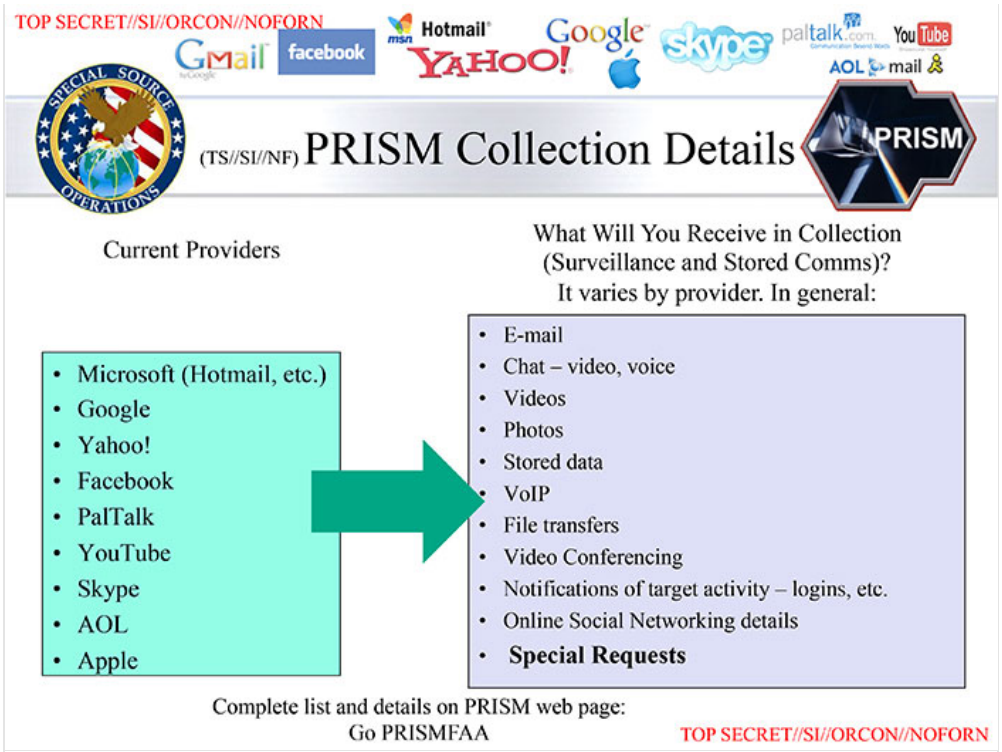
Monitoring a target's communication

This diagram shows how the bulk of the world's electronic communications move through companies based in the United States.



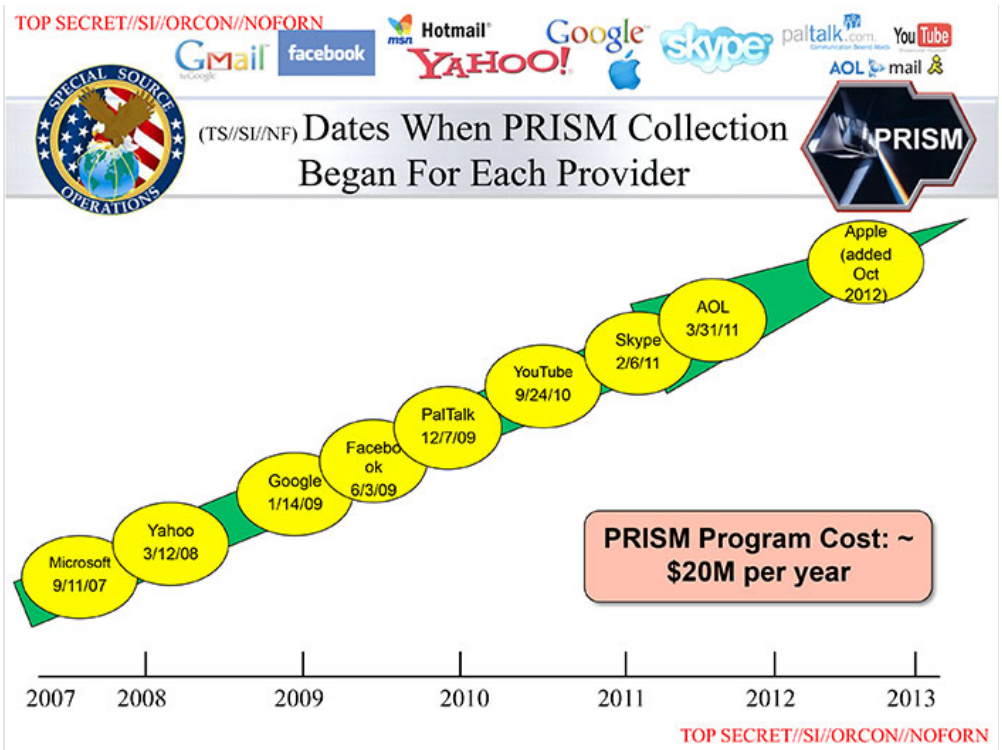
Providers and data

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.



Jonathan Qiang Li
7/15/2013 6:47 PM MST

Osama Bin Laden may be laughing in his tomb that he has finally achieved his purpose: terrorize Americans in their daily living. He achieved this by getting into American's head.

Liked by 1 reader Reply

daniel Boemo
7/12/2013 6:39 PM MST

Interestingly, the last bombing in his country, his government was warned about terrorists by the Russians. What actually happens is to show that the same holds information not knowing what to do with it.

Liked by 1 reader Reply

unitedstasiofamerica
7/12/2013 4:25 AM MST

United Stasi of America:
http://apps.opendatacity.de/stasi-vs-nsa/english.h...

Reply

Sharon Akins
7/11/2013 9:42 PM MST

I am a stay at home writer trying to break into print with my own novels. I like them to be as real world as I can and do a LOT of research on my subject matter. Right now my research has been pretty safe, but God forbid I ever get an idea for a story about a bomber or any other intrigue or espionage story plot because I'd be labeled a terrorist just by doing research for a fiction novel.

Reply

Liston Tome
7/11/2013 9:02 AM MST

Is there a terrorist under every bed in America? Of course not except in the imaginations of bureaucrats and profiteers that want expanded powers and government budgets.
The US has real problems to solve. If we could only blame everything on terrorists maybe the government would do something to solve the real problems that are killing Americans.
Lack of health care is killing Americans. Poor education is killing Americans. The proliferation of guns is killing Americans. The lack of jobs is ... **See More**

Liked by 2 readers Reply

David M. Higgins
7/11/2013 1:44 PM MST

A 'Terrorist' is now defined as an 'Enemy of the State' regardless of whether or not they have ever used the Asymmetrical Warfare tactic of Terrorism. The Government defines Enemy of the State as anyone or anything that is in opposition to its purposes - secret or stated. Therefore like in the George Orwell book '1984' - Big Brother seeks to keep surveillance on its own people with an END of maintaining, "a BOOT on a Human Face - Forever"

Liked by 2 readers

View -1 more reply

Add your thoughts...

LOAD MORE COMMENTS

Rachel Weiner
Little support on either side of the aisle for a boycott.

Obama's Moscow visit to meet Putin is in limbo because of Snowden standoff

FISA court seeks release of declassified filings in secret Yahoo case

More furloughed feds requesting aid, official says

What Should Edward "I'm a Brave Martyr But I Wanna Go Home" Snowden Do Now?

At Commerce Dept., false alarm on cyberattack cost almost $3 million

James Comey confirmation hearing: Live updates