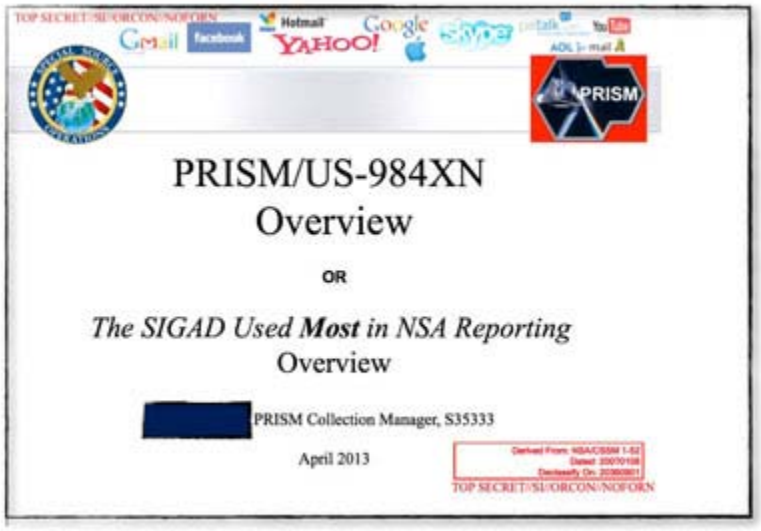
theguardian

NSA taps in to internet giants' systems to mine user data, secret files reveal

• Top secret PRISM program claims direct access to servers of firms including Google, Facebook and Apple

• Companies deny any knowledge of program in operation since 2007

Glenn Greenwald and Ewen MacAskill
The Guardian, Thursday 6 June 2013 18.05 EDT



A slide depicting the top-secret PRISM program

The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian.

The NSA access is part of a previously undisclosed program called PRISM, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says.

The Guardian has verified the authenticity of the document, a 41-slide PowerPoint presentation – classified as top secret with no distribution to foreign allies – which was apparently used to train intelligence operatives on the capabilities of the program. The document claims "collection directly from the servers" of major US service providers.

Although the presentation claims the program is run with the assistance of the companies, all those who responded to a Guardian request for comment on Thursday denied knowledge of any such program.

In a statement, Google said: "Google cares deeply about the security of our users' data. 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."

Several senior tech executives insisted that they had no knowledge of PRISM or of any similar scheme. They said they would never have been involved in such a program. "If they are doing this, they are doing it without our knowledge," one said.

An Apple spokesman said it had "never heard" of PRISM.

The NSA access was enabled by changes to US surveillance law introduced under President Bush and renewed under Obama in December 2012.

The program facilitates extensive, in-depth surveillance on live communications and stored information. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.

It also opens the possibility of communications made entirely within the US being collected without warrants.

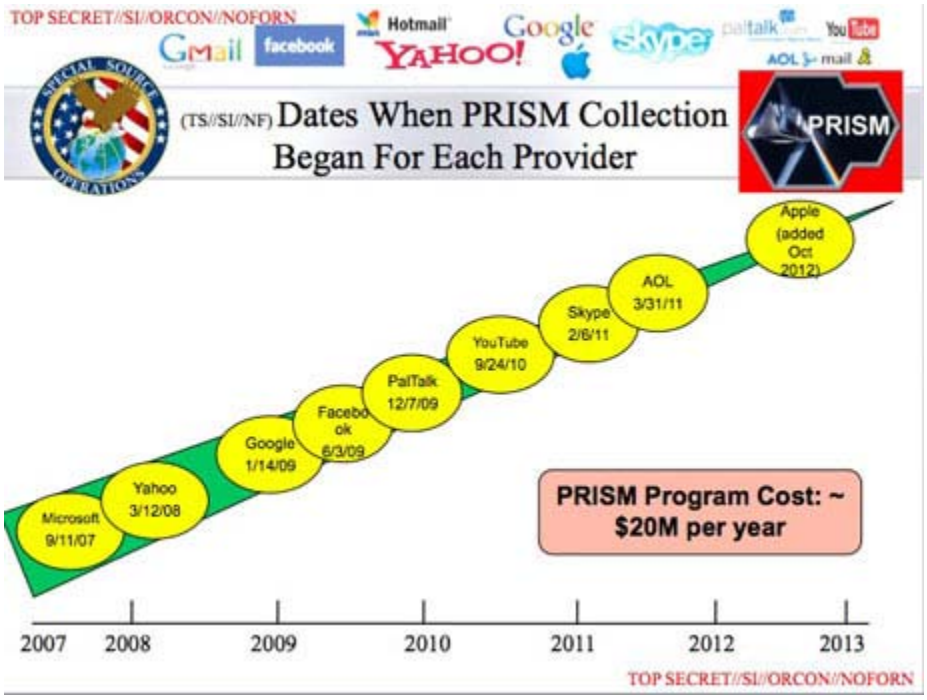
Disclosure of the PRISM program follows a leak to the Guardian on Wednesday of a top-secret court order compelling telecoms provider Verizon to turn over the telephone records of millions of US customers.

The participation of the internet companies in PRISM will add to the debate, ignited by the Verizon revelation, about the scale of surveillance by the intelligence services. Unlike the collection of those call records, this surveillance can include the content of communications and not just the metadata.

Some of the world's largest internet brands are claimed to be part of the information-sharing program since its introduction in 2007. Microsoft – which is currently running an advertising campaign with the slogan "Your privacy is our priority" – was the first, with collection beginning in December 2007.

It was followed by Yahoo in 2008; Google, Facebook and PalTalk in 2009; YouTube in 2010; Skype and AOL in 2011; and finally Apple, which joined the program in 2012. The program is continuing to expand, with other providers due to come online.

Collectively, the companies cover the vast majority of online email, search, video and communications networks.



The extent and nature of the data collected from each company varies.

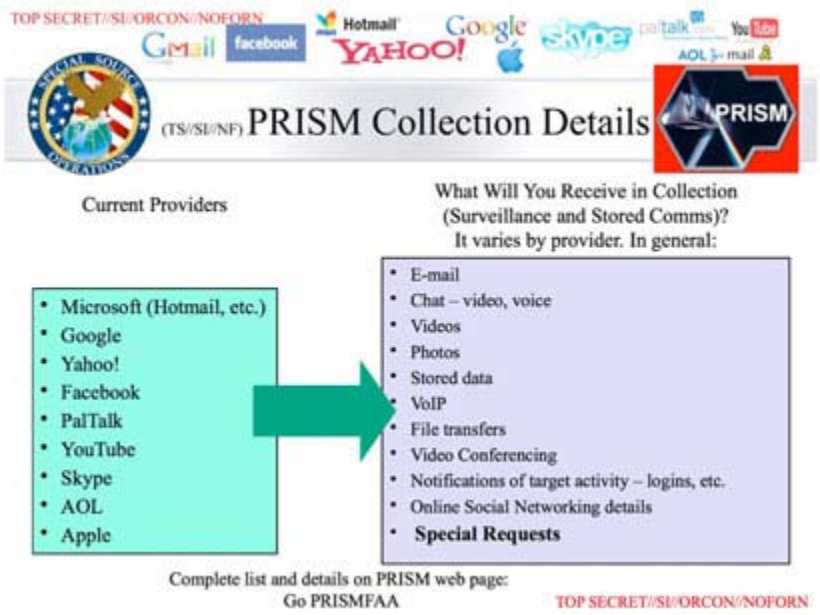
Companies are legally obliged to comply with requests for users' communications under US law, but the PRISM program allows the intelligence services direct access to the companies' servers. The NSA document notes the operations have "assistance of communications providers in the US".

The revelation also supports concerns raised by several US senators during the renewal of the Fisa Amendments Act in December 2012, who warned about the scale of surveillance the law might enable, and shortcomings in the safeguards it introduces.

When the FAA was first enacted, defenders of the statute argued that a significant check on abuse would be the NSA's inability to obtain electronic communications without the consent of the telecom and internet companies that control the data. But the PRISM program renders that

consent unnecessary, as it allows the agency to directly and unilaterally seize the communications off the companies' servers.

A chart prepared by the NSA, contained within the top-secret document obtained by the Guardian, underscores the breadth of the data it is able to obtain: email, video and voice chat, videos, photos, voice-over-IP (Skype, for example) chats, file transfers, social networking details, and more.



The document is recent, dating to April 2013. Such a leak is extremely rare in the history of the NSA, which prides itself on maintaining a high level of secrecy.

The PRISM program allows the NSA, the world's largest surveillance organisation, to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.

With this program, the NSA is able to reach directly into the servers of the participating companies and obtain both stored communications as well as perform real-time collection on targeted users.

The presentation claims PRISM was introduced to overcome what the NSA regarded as shortcomings of Fisa warrants in tracking suspected foreign terrorists. It noted that the US has a "home-field advantage" due to housing much of the internet's architecture. But the presentation claimed "Fisa constraints restricted our home-field advantage" because Fisa required individual warrants and confirmations that both the sender and receiver of a communication were outside the US.

"Fisa was broken because it provided privacy protections to people who were not entitled to them," the presentation claimed. "It took a Fisa court order to collect on foreigners overseas who were communicating with other foreigners overseas simply because the government was collecting off a wire in the United States. There were too many email accounts to be practical to seek Fisas for all."

The new measures introduced in the FAA redefines "electronic surveillance" to exclude anyone "reasonably believed" to be outside the USA – a technical change which reduces the bar to initiating surveillance.

The act also gives the director of national intelligence and the attorney general power to permit obtaining intelligence information, and indemnifies internet companies against any actions arising as a result of co-operating with authorities' requests.

In short, where previously the NSA needed individual authorisations, and confirmation that all parties were outside the USA, they now need only reasonable suspicion that one of the parties was outside the country at the time of the records were collected by the NSA.

The document also shows the FBI acts as an intermediary between other agencies and the tech companies, and stresses its reliance on the participation of US internet firms, claiming "access is 100% dependent on ISP provisioning".

In the document, the NSA hails the PRISM program as "one of the most valuable, unique and productive accesses for NSA".

It boasts of what it calls "strong growth" in its use of the PRISM program to obtain communications. The document highlights the number of obtained communications increased in 2012 by 248% for Skype – leading the notes to remark there was "exponential growth in Skype reporting; looks like the word is getting out about our capability against Skype". There was also a 131% increase in requests for Facebook data, and 63% for Google.

The NSA document indicates that it is planning to add Dropbox as a PRISM provider. The agency also seeks, in its words, to "expand collection services from existing providers".

The revelations echo fears raised on the Senate floor last year during the expedited debate on the renewal of the FAA powers which underpin the PRISM program, which occurred just days before the act expired.

Senator Christopher Coons of Delaware specifically warned that the secrecy surrounding the various surveillance programs meant there was no way to know if safeguards within the act were working.

"The problem is: we here in the Senate and the citizens we represent don't know how well any of these safeguards actually work," he said.

"The law doesn't forbid purely domestic information from being collected. We know that at least one Fisa court has ruled that the surveillance program violated the law. Why? Those who know can't say and average Americans can't know."

Other senators also raised concerns. Senator Ron Wyden of Oregon attempted, without success, to find out any information on how many phone calls or emails had been intercepted under the program.

When the law was enacted, defenders of the FAA argued that a significant check on abuse would be the NSA's inability to obtain electronic communications without the consent of the telecom and internet companies that control the data. But the PRISM program renders that consent unnecessary, as it allows the agency to directly and unilaterally seize the communications off the companies' servers.

When the NSA reviews a communication it believes merits further investigation, it issues what it calls a "report". According to the NSA, "over 2,000 PRISM-based reports" are now issued every month. There were 24,005 in 2012, a 27% increase on the previous year.

In total, more than 77,000 intelligence reports have cited the PRISM program.

Jameel Jaffer, director of the ACLU's Center for Democracy, that it was astonishing the NSA would even ask technology companies to grant direct access to user data.

"It's shocking enough just that the NSA is asking companies to do this," he said. "The NSA is part of the military. The military has been granted unprecedented access to civilian communications.

"This is unprecedented militarisation of domestic communications infrastructure. That's profoundly troubling to anyone who is concerned about that separation."

A senior administration official said in a statement: "The Guardian and Washington Post articles refer to collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act. This law does not allow the targeting of any US citizen or of any person located within the United States.

"The program is subject to oversight by the Foreign Intelligence Surveillance Court, the Executive Branch, and Congress. It involves extensive procedures, specifically approved by the court, to ensure that only non-US persons outside the US are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about US persons.

"This program was recently reauthorized by Congress after extensive hearings and debate.

"Information collected under this program is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats.

"The Government may only use Section 702 to acquire foreign intelligence information, which is specifically, and narrowly, defined in the Foreign Intelligence Surveillance Act. This requirement applies across the board, regardless of the nationality of the target."

Additional reporting by James Ball and Dominic Rushe

http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data