Prism Exposed: Data Surveillance with Implications for the World

The article you are reading originally appeared in German in issue 24/2013 (June 10, 2013) of DER SPIEGEL.

By Marcel Rosenbach, Holger Stark and Jonathan Stock

AP

The American intelligence director and the White House have finally confirmed what insiders have long known: The Obama administration is spying on the entire world. Politicians in Germany are demanding answers.

South of Utah's Great Salt Lake, the National Security Agency (NSA), a United States foreign intelligence service, keeps watch over one of its most expensive secrets. Here, on 100,000 square meters (1,100,000 square feet) near the US military's Camp Williams, the NSA is constructing enormous buildings to house superfast computers. All together, the project will cost around $2 billion (€1.5 billion) and the computers will be capable of storing a gigantic volume of data, at least 5 billion gigabytes. The energy needed to power the cooling system for the servers alone will cost $40 million a year.

Former NSA employees Thomas Drake and Bill Binney told SPIEGEL in March that the facility would soon store personal data on people from all over the world and keep it for decades. This includes emails, Skype conversations, Google searches, YouTube videos, Facebook posts, bank transfers -- electronic data of every kind.

"They have everything about you in Utah," Drake says. "Who decides whether they look at that data? Who decides what they do with it?" Binney, a mathematician who was previously an influential analyst at the NSA, calculates that the servers are large enough to store the entirety of humanity's electronic communications for the next 100 years -- and that, of course, gives his former colleagues plenty of opportunity to read along and listen in.

James Clapper, the country's director of national intelligence, has confirmed the existence of a large-scale surveillance program. President Barack Obama further explained that Congress authorized the program -- but that American citizens are exempt from it.

A top-secret document published last week by the *Washington Post* and Britain's *Guardian* shows where the NSA may be getting the majority of its data. According to the document, which was allegedly leaked by former CIA employee Edward Snowden, the intelligence agency began seeking out direct access to servers belonging to American Internet companies on a wide scale in 2007. The first of these companies to come onboard was Microsoft. Yahoo followed half a year later, then Google, Facebook, PalTalk, YouTube, Skype and AOL. The most recent company to declare its willingness to cooperate was Apple, in October 2012, according to the secret government document, which proudly states that this access to data is achieved "directly from the servers" of the companies.

The companies in question denied that claim on Friday. But if what the document says is true, the NSA has the potential to know what every person in the world who uses these companies' services is doing, and that presumably includes millions of Germans.

'Total Surveillance of Germans is Inappropriate'

On Monday, German Chancellor Angela Merkel confirmed through a spokesman that she plans to discuss the NSA's controversial data surveillance program with President Obama during his visit to Berlin next week. A spokesperson for the German Justice Ministry also said that talks are currently underway with US authorities. The discussions will include implications to Germany and "possible impairment of the rights of German citizens."

German Consumer Protection Minister Ilse Aigner has called for "clear answers" from the companies implicated in the document, and the German Green Party has demanded that the government investigate the circumstances of Prism immediately.

"Total surveillance of all German citizens by the NSA is completely disproportionate," Volker Beck, secretary of the Green Party group in parliament, said on Monday. The party has proposed that the topic be discussed at next week's parliamentary session.

Mormon Roots, International Reach

The program's Utah compound is full of security fences, watchdogs and surveillance cameras, as well as biometric identification system equipment. Two informants say the location for the server facility was by no means an accident. Utah is home to the largest number of Mormons in the world. This highly patriotic religious community sends its young members around the world as missionaries -- and many are then recruited by the Utah Army National Guard, whose 300th Military Intelligence Brigade employs 1,600 linguists. The NSA has access to these linguists at all times, and one insider believes they are used in "analyzing international telecommunications."

In the secret document, the NSA's surveillance program is referred to by the name "Prism." A prism is also the shape that reflects light in fiber optic cables -- the same cables that form the backbone of the world's Internet traffic. The document, which was authored for an internal NSA presentation, shows that even data streams traveling from Europe to Asia, the Pacific region or South America often pass through servers in the US. "A target's phone call, email or chat will take the cheapest path, not the physically most direct path," the document reads.

The Bush administration legalized this new dimension to government snooping, but it was the Obama administration that renewed the law in question in December 2012. The law permits, for example, the surveillance of all Google users not living in the US, as well as communications between American citizens and people in other countries.

Broadened Legal Basis for Spying

The document also shows that with programs such as Prism, the NSA is reinterpreting the legal basis for its actions on one crucial point. For decades, intelligence services required an order from a special court with precise specifications on their suspect if they wanted to monitor an email account, for example. Now, it's enough if the NSA has reasonable evidence that a subject is either living abroad or communicating with someone who lives outside the US. This expands the circle of potential suspects, lowers bureaucratic hurdles and reduces democratic checks and balances, making it even easier and faster to gather data on even more people.

The NSA's data collection powers extend far beyond American Internet servers. The agency also conducts reconnaissance around the globe, for example with satellites. It has also installed high-performance antennae in various countries to pick up mobile phone communications. Never before has a government collected data on such a large scale.

The NSA is a useful partner for German authorities. The director of the NSA, four-star General Keith Alexander, regularly receives delegations from Germany at his headquarters at Fort Meade. These meetings are generally constructive, in part because the pecking order is clear: The NSA nearly always knows much more, while the Germans act as assistants. Germany's foreign intelligence agency, the BND, conducts various secret operations in tandem with the NSA, most of them concerning large-scale data collection. German authorities have also helped the American security agency with a number of activities, especially in regions in crisis.

For its part, the NSA regularly shares with Germany's security agencies the leads it has on suspects. A 2007 bomb plot by an Islamist terror cell in Germany, the so-called Sauerland group, was discovered because of emails and telephone conversations that the NSA monitored and passed along to its German counterparts.

According to former NSA employee Binney, American programs have also been used in Germany, although a former high-ranking security official in the country says German authorities were not involved in the Prism program.

It is now clear that what experts suspected for years is in fact true -- that the NSA monitors every form of electronic communication around the globe. This fact raises an important question: How can an intelligence agency, even one as large and well-staffed as the NSA with its 40,000 employees, work meaningfully with such a flood of information?

The answer to this question is part of a phenomenon that is currently a major topic for the business community as well and goes by the name "Big Data." Thanks to new database technologies, it is now possible to connect entirely disparate forms of data and analyze them automatically.

A rare glimpse into what intelligence services can do by applying this "big data" approach came last year from David Petraeus. This new form of data analysis is concerned with discovering "non-obvious relationships," the then freshly minted CIA director explained at a conference. This includes, for example "finding connections between a purchase here, a phone call there, a grainy video, customs and immigration information."

The goal, according to Petraeus, is for big data to "lead to automated discovery, rather than depending on the right analyst asking the right question." Algorithms pick out connections automatically from the unstructured sea of data they trawl. "The CIA and our intelligence community partners must be able to swim in the ocean of 'Big Data.' Indeed, we must be world class swimmers -- the best, in fact," the CIA director continued.

The Surveillance State

The value of big data analysis for US intelligence agencies can be seen in the amount the NSA and CIA are investing in it. Not only does this include multimillion-dollar contracts with providers specializing in data mining services, but the CIA also invests directly, through its subsidiary company In-Q-Tel, in several big data start-ups.

It's about rendering people and their behavior predictable. The NSA's research projects aim to forecast, on the basis of telephone data and Twitter and Facebook posts, when uprisings, social protests and other events will occur. The agency is also researching new methods of analysis for surveillance videos with the hopes of recognizing conspicuous behavior before an attack is committed.

Gus Hunt, the CIA's chief technology officer, made a forthright admission in March: "We fundamentally try to collect everything and hang onto it forever." What he meant by "everything," Hunt also made clear: "It is really very nearly within our grasp to be able to compute on all human-generated information," he said.

That statement is difficult to reconcile with the Fourth Amendment to the US Constitution, which guarantees the right to privacy. This is probably why Hunt added, almost apologetically: "Technology in this world is moving faster than government or law can keep up."

Translated from the German by Ella Ornstein