

Global surveillance

Global surveillance refers to the mass surveillance of entire populations across national borders.^[1] Its roots can be traced back to the middle of the 20th century when the UKUSA Agreement was jointly enacted by the United Kingdom and the United States, which later expanded to Canada, Australia, and New Zealand to create the present Five Eyes alliance. The alliance developed cooperation arrangements with several "third-party" nations. Eventually, this resulted in the establishment of a global surveillance network, code-named "ECHELON" (1971).^{[2][3]}

Its existence, however, was not widely acknowledged by governments and the mainstream media until the global surveillance disclosures by Edward Snowden triggered a debate about the right to privacy in the Digital Age.^{[4][5]}

Contents

Historical background

Snowden's disclosures

By category

Purposes

Targets and methods

- Collection of metadata and other content
- Contact chaining
- Data transfer
- Financial payments monitoring
- Mobile phone location tracking
- Infiltration of smartphones
- Infiltration of commercial data centers
- Infiltration of anonymous networks
- Monitoring of hotel reservation systems
- Virtual reality surveillance

Political espionage

International cooperation

- Australia
- Canada
- Denmark
- France
- Germany
- Israel
- Japan
- Libya
- Netherlands
- Norway
- Singapore
- Spain
- Sweden
- Switzerland
- United Kingdom
- United States

Commercial cooperation

- AT&T
- Booz Allen Hamilton
- British Telecommunications
- Microsoft
- Orange S.A.
- RSA Security
- Stratfor
- Vodafone
- In-Q-Tel

Palantir Technologies

Surveillance evasion

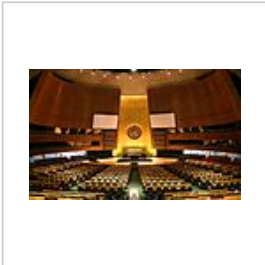
- North Korea
- Iran
- Libya

Impact

See also

References

Further reading



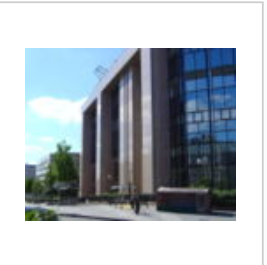
According to Snowden's documents, the United Nations Headquarters and the United Nations General Assembly were targeted by NSA employees disguised as diplomats.^[6]



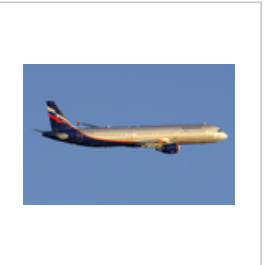
Citing Snowden's documents, The Guardian reported that British officials had set up fake Internet cafes at the 2009 G-20 London summit to spy on the delegates' use of computers, and to install key-logging software on the delegates' phones. This allowed British representatives to gain a "negotiating advantage" at the summit.^[7]



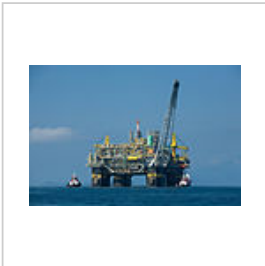
According to Snowden's interview with the South China Morning Post, the U.S. government has been hacking numerous non-military targets in China for years. Other high-priority targets include academic institutions such as the prestigious Tsinghua University in Beijing.^[8]



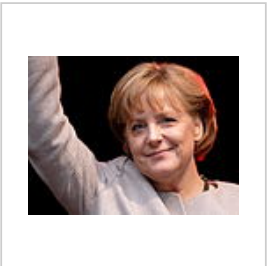
The Council of the European Union, with its headquarters at the Justus Lipsius building in Brussels, was targeted by NSA employees working near the headquarters of NATO. An NSA document dated September 2010 explicitly names the Europeans as a "location target".^[9]



The reservations system of Russia's Aeroflot airline was hacked by the NSA.^[10]



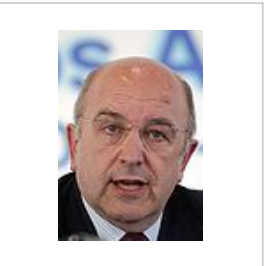
Petrobras, currently the world's leader in offshore deepwater drilling, is a "prominent" target of the U.S. government.^[11]



From 2002 to 2013, the German Chancellor Angela Merkel was targeted by the U.S. Special Collection Service.^[12]



Israeli Prime Minister Ehud Olmert (pictured) and Defense Minister Ehud Barak were included in a list of surveillance targets used by the GCHQ and the NSA.^[13]



Joaquín Almunia, who served as the European Commissioner for Competition and the Vice-President of the European Commission, was targeted by Britain's GCHQ agency.^[14]



Indonesia's President Susilo Bambang Yudhoyono and his wife were placed under surveillance by the Australian Signals Directorate (ASD).^[15] During the 2007 United Nations Climate Change Conference in Bali, the ASD cooperated with the NSA to conduct mass surveillance on the Indonesian hosts.^[16]



The video gaming network Xbox Live was placed under surveillance to unravel possible terrorist plots.^[17]

Historical background

The origins of global surveillance can be traced back to the late 1940s after the UKUSA Agreement was collaboratively enacted by the United Kingdom and the United States, which eventually culminated in the creation of the global surveillance network code-named "**ECHELON**" in 1971.^{[2][3]}

In the aftermath of the 1970s Watergate affair and a subsequent congressional inquiry led by Sen. Frank Church,^[18] it was revealed that the NSA, in collaboration with Britain's GCHQ, had routinely intercepted the international communications of prominent anti-Vietnam War leaders such as Jane Fonda and Dr. Benjamin Spock.^[19] Decades later, a multi-year investigation by the European Parliament highlighted the NSA's role in economic espionage in a report entitled 'Development of Surveillance Technology and Risk of Abuse of Economic Information', in 1999.^[20]

However, for the general public, it was a series of detailed disclosures of internal NSA documents in June 2013 that first revealed the massive extent of the NSA's spying, both foreign and domestic. Most of these were leaked by an ex-contractor, Edward Snowden. Even so, a number of these older global surveillance programs such as PRISM, XKeyscore, and Tempora were referenced in the 2013 release of thousands of documents.^[21] Many countries around the world, including Western Allies and member states of NATO, have been targeted by the "Five Eyes" strategic alliance of Australia, Canada, New Zealand, the UK and the USA—five English-speaking Western countries aiming to achieve Total Information Awareness by mastering the Internet with analytical tools such as the Boundless Informant.^[22] As confirmed by the NSA's director Keith B. Alexander on 26 September 2013, the NSA collects and stores all phone records of all American citizens.^[23] Much of the data is kept in large storage facilities such as the Utah Data Center, a US\$1.5 billion megaproject referred to by *The Wall Street Journal* as a "symbol of the spy agency's surveillance prowess."^[24]

Today, this global surveillance system continues to grow. It now collects so much digital detritus — e-mails, calls, text messages, cellphone location data and a catalog of computer viruses - that the N.S.A. is building a 1-million-square-foot facility in the Utah desert to store and process it.

— *The New York Times*^[25] (August 2012)

On 6 June 2013, Britain's *The Guardian* newspaper began publishing a series of revelations by an as yet unknown American whistleblower, revealed several days later to be ex-CIA and ex-NSA-contracted systems analyst Edward Snowden. Snowden gave a cache of documents to two journalists: Glenn Greenwald and Laura Poitras, Greenwald later estimated that the cache contains 15,000 – 20,000 documents, some very large and very detailed, and some very small.^{[26][27]} In over two subsequent months of publications, it became clear that the NSA had operated a complex web of spying programs which allowed it to intercept Internet and telephone conversations from over a billion users from dozens of countries around the world. Specific revelations were made about China, the European Union, Latin America, Iran and Pakistan, and Australia and New Zealand, however, the published documentation reveals that many of the programs indiscriminately collected bulk information directly from central servers and Internet backbones, which almost invariably carry and reroute information from distant countries.

Due to this central server and backbone monitoring, many of the programs overlapped and interrelated among one another. These programs were often carried out with the assistance of US entities such as the United States Department of Justice and the FBI,^[28] was sanctioned by US laws such as the FISA Amendments Act, and the necessary court orders for them were signed by the secret Foreign

Intelligence Surveillance Court. Some of the NSA's programs were directly aided by national and foreign intelligence agencies, Britain's GCHQ and Australia's DSD, as well as by large private telecommunications and Internet corporations, such as Verizon, Telstra,^[29] Google and Facebook.^[30]

Snowden's disclosures of the NSA's surveillance activities are a continuation of news leaks which have been ongoing since the early 2000s. One year after the September 11, 2001, attacks, former U.S. intelligence official William Binney, was publicly critical of the NSA for spying on U.S. citizens.^[31]

Further disclosures followed. On 16 December 2005, The New York Times published a report under the headline "Bush Lets U.S. Spy on Callers Without Courts".^[32] In 2006, further evidence of the NSA's domestic surveillance of U.S. citizens was provided by USA Today. The newspaper released a report on 11 May 2006, regarding the NSA's "massive database" of phone records collected from "tens of millions" of U.S. citizens. According to USA Today, these phone records were provided by several telecom companies such as AT&T, Verizon and BellSouth.^[33] In 2008, the security analyst Babak Pashar revealed the existence of the so-called "Quantico circuit" that he and his team discovered in 2003 when brought on to update the carrier's security system. The circuit provided the U.S. federal government with a backdoor into the network of an unnamed wireless provider, which was later independently identified as Verizon.^[34]

Snowden's disclosures

Snowden made his first contact with journalist Glenn Greenwald of The Guardian in late 2012.^[35] The timeline of mass surveillance disclosures by Snowden continued throughout the entire year of 2013.

By category

Documents leaked by Snowden in 2013 include court orders, memos, and policy documents related to a wide range of surveillance activities.

Purposes

According to the April 2013 summary of documents leaked by Snowden, other than to combat terrorism, these surveillance programs were employed to assess the foreign policy and economic stability of other countries,^[36] and to gather "commercial secrets".^[37]

In a statement addressed to the National Congress of Brazil in early August 2013, journalist Glenn Greenwald maintained that the U.S. government had used counter-terrorism as a pretext for clandestine surveillance in order to compete with other countries in the "business, industrial and economic fields".^[38]^[39]^[40] In a December 2013 letter to the Brazilian government, Snowden wrote that "These programs were never about terrorism: they're about economic spying, social control, and diplomatic manipulation. They're about power".^[41] According to White House panel member NSA didn't stop any terrorist attack.^[42] However NSA chief said, that surveillance programs stopped 54 terrorist plots.^[43]

In an interview with Der Spiegel published on 12 August 2013, former NSA Director Michael Hayden admitted that "We (the NSA) steal secrets. We're number one in it". Hayden also added: "We steal stuff to make you safe, not to make you rich".^[36]

According to documents seen by the news agency Reuters, these "secrets" were subsequently funnelled to authorities across the nation to help them launch criminal investigations of Americans.^[44] Federal agents are then instructed to "recreate" the investigative trail in order to "cover up" where the information originated.^[44]

According to the congressional testimony of Keith B. Alexander, Director of the National Security Agency, one of the purposes of its data collection is to store all the phone records inside a place that can be searched and assessed at all times. When asked by Senator Mark Udall if the goal of the NSA is to collect the phone records of all Americans, Alexander replied, "Yes, I believe it is in the nation's best interest to put all the phone records into a lockbox that we could search when the nation needs to do it."^[45]

Targets and methods

Collection of metadata and other content

In the United States, the NSA is collecting the phone records of more than 300 million Americans.^[46] The international surveillance tool **XKeyscore** allows government analysts to search through vast databases containing emails, online chats and the browsing histories of millions of individuals.^[47]^[48]^[49] Britain's global surveillance program **Tempora** intercepts the fibre-optic cables that form the

In order to decode private conversations, the NSA has cracked the most commonly used cellphone encryption technology, A5/1. According to a classified document leaked by Snowden, the agency can "process encrypted A5/1" even when it has not acquired an encryption key.^[64] In addition, the NSA uses various types of cellphone infrastructure, such as the links between carrier networks, to determine the location of a cellphone user tracked by Visitor Location Registers.^[65]

Infiltration of smartphones

As worldwide sales of smartphones grew rapidly, the NSA decided to take advantage of the smartphone boom. This is particularly advantageous because the smartphone contains a variety of data sets that would interest an intelligence agency, such as social contacts, user behaviour, interests, location, photos and credit card numbers and passwords.^[66]

According to the documents leaked by Snowden, the NSA has set up task forces assigned to several smartphone manufacturers and operating systems, including Apple Inc.'s iPhone and iOS operating system, as well as Google's Android mobile operating system.^[66] Similarly, Britain's GCHQ assigned a team to study and crack the BlackBerry.^[66] In addition, there are smaller NSA programs, known as "scripts", that can perform surveillance on 38 different features of the iOS 3 and iOS 4 operating systems. These include the mapping feature, voicemail and photos, as well as Google Earth, Facebook and Yahoo! Messenger.^[66]

Infiltration of commercial data centers

In contrast to the **PRISM** surveillance program, which is a front-door method of access that is nominally approved by the FISA court, the **MUSCULAR** surveillance program is noted to be "unusually aggressive" in its usage of unorthodox hacking methods to infiltrate Yahoo! and Google data centres around the world. As the program is operated overseas (United Kingdom), the NSA presumes that anyone using a foreign data link is a foreigner, and is, therefore, able to collect content and metadata on a previously unknown scale from U.S. citizens and residents.^[67] According to the documents leaked by Snowden, the MUSCULAR surveillance program is jointly operated by the NSA and Britain's GCHQ agency.^[68] (See International cooperation.)

Infiltration of anonymous networks

The Five Eyes have made repeated attempts to spy on Internet users communicating in secret via the anonymity network Tor. Several of their clandestine operations involve the implantation of malicious code into the computers of anonymous Tor users who visit infected websites. In some cases, the NSA and GCHQ have succeeded in blocking access to the anonymous network, diverting Tor users to insecure channels. In other cases, the NSA and the GCHQ were able to uncover the identity of these anonymous users.^{[69][70][71][72][73][74][75][76][77]}

Monitoring of hotel reservation systems

Under the **Royal Concierge** surveillance program, Britain's GCHQ agency uses an automated monitoring system to infiltrate the reservation systems of at least 350 luxury hotels in many different parts of the world.^[78] Other related surveillance programs involve the wiretapping of room telephones and fax machines used in targeted hotels, as well as the monitoring of computers, hooked up to the hotel network.^[78]

Virtual reality surveillance

The U.S. National Security Agency (NSA), the U.S. Central Intelligence Agency (CIA), and Britain's Government Communications Headquarters (GCHQ) have been conducting surveillance on the networks of many online games, including massively multiplayer online role-playing games (MMORPGs) such as World of Warcraft, as well as virtual worlds such as Second Life, and the Xbox gaming console.^[79]

Political espionage









According to the April 2013 summary of disclosures, the NSA defined its "intelligence priorities" on a scale of "1" (highest interest) to "5" (lowest interest).^[36] It classified about 30 countries as "3rd parties", with whom it cooperates but also spies on:

- **Main targets:** China, Russia, Iran, Pakistan and Afghanistan were ranked highly on the NSA's list of spying priorities, followed by France, Germany, Japan, and Brazil. The European Union's "international trade" and "economic stability" are also of interest.^[36] Other high priority targets include Cuba, Israel, and North Korea.^[80]
- **Irrelevant:** From a US intelligence perspective, countries such as Cambodia, Laos and Nepal were largely irrelevant, as were governments of smaller European Union countries such as Finland, Denmark, Croatia and the Czech Republic.^[36]

Other prominent targets included members and adherents of the Internet group known as "Anonymous",^[36] as well as potential whistleblowers.^[81] According to Snowden, the NSA targeted reporters who wrote critically about the government after 9/11.^[82]

As part of a joint operation with the Central Intelligence Agency (CIA), the NSA deployed secret eavesdropping posts in eighty U.S. embassies and consulates worldwide.^[6] The headquarters of NATO were also used by NSA experts to spy on the European Union.^[83]

In 2013, documents provided by Edward Snowden revealed that the following intergovernmental organizations, diplomatic missions, and government ministries have been subjected to surveillance by the "Five Eyes":

Country/ Organization	Target	Method(s)
 <u>Brazil</u>	<u>Ministry of Energy</u>	Collection of <u>metadata</u> records by the <u>Communications Security Establishment of Canada</u> (CSEC) ^[84]
 <u>France</u>	<u>Ministry of Foreign and European Affairs</u>	Infiltration of <u>virtual private networks</u> (VPN) ^[85]
	<u>Embassy of France in Washington, D.C.</u>	
 <u>Germany</u>	<u>Embassy of Germany in Rwanda</u> ^[14]	
 <u>Italy</u>	<u>Embassy of Italy in Washington, D.C.</u>	<ul style="list-style-type: none"> Installation of <u>physical implants</u>^[86] Copying of entire <u>hard disk drives</u>^[86]
 <u>India</u>	<u>Embassy of India in Washington, D.C.</u>	<ul style="list-style-type: none"> Copying entire <u>hard disk drives</u>^[87] Picking data from <u>screenshots</u>^[87]
	<u>Permanent Representative of India to the United Nations</u>	
 <u>Mexico</u>	<u>Secretariat of Public Security</u>	<ul style="list-style-type: none"> Hacking of e-mail accounts as part of an operation code-named "<u>Whitetamale</u>"^[88]
 <u>European Union</u>	<u>Council of the European Union in Brussels</u>	<ul style="list-style-type: none"> Installation of <u>covert listening devices</u>^[89] Hacking and infiltration of <u>virtual private networks</u>^[90] <u>Disk cloning</u>^[90]
	<u>Delegation to the United Nations in New York</u>	
	<u>Delegation to the United States in Washington, D.C.</u>	
 <u>United Nations</u>	<u>United Nations Headquarters</u>	<ul style="list-style-type: none"> Hacking of encrypted communications^[90] Infiltration of internal <u>video conferences</u>^[90]
	<u>International Atomic Energy Agency (IAEA)</u>	
	<u>United Nations Development Programme (UNDP)</u> ^[14]	
	<u>United Nations Children's Fund (UNICEF)</u> ^[14]	





International cooperation


During World War II, the BRUSA Agreement was signed by the governments of the United States and the United Kingdom for the purpose of intelligence sharing.^[91] This was later formalized in the UKUSA Agreement of 1946 as a secret treaty. The full text of the agreement was released to the public on 25 June 2010.^[92]

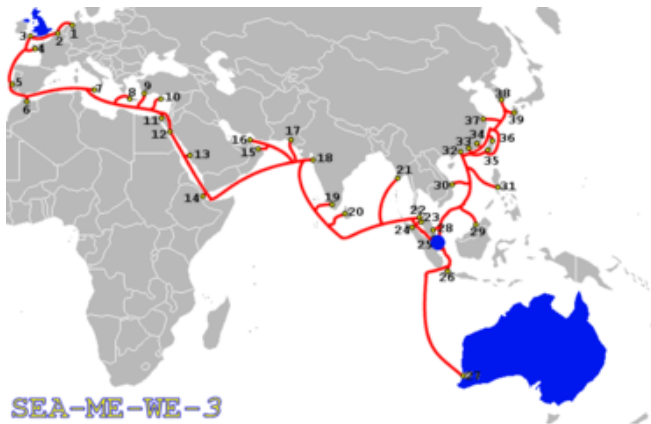
Although the treaty was later revised to include other countries such as Denmark, Germany, Ireland, Norway, Turkey, and the Philippines,^[92] most of the information sharing has been performed by the so-called "**Five Eyes**",^[93] a term referring to the following English-speaking western democracies and their respective intelligence agencies:



The "Five Eyes" of Australia, Canada, New Zealand, the United Kingdom and the United States

-  – The Defence Signals Directorate of Australia^[93]
-  – The Communications Security Establishment of Canada^[93]
-  – The Government Communications Security Bureau of New Zealand^[93]
-  – The Government Communications Headquarters of the United Kingdom, which is widely considered to be a leader in traditional spying due to its influence on countries that were once part of the British Empire.^[93]

-  – The National Security Agency of the United States, which has the biggest budget and the most advanced technical abilities among the "*five eyes*".^[93]

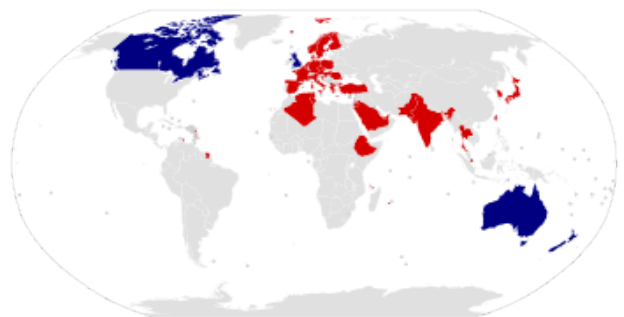


Top secret documents leaked by Snowden revealed that the "Five Eyes" have gained access to the majority of Internet and telephone communications flowing throughout Europe, the United States, and other parts of the world.

Left: SEA-ME-WE 3, which runs across the Afro-Eurasian supercontinent from Japan to Northern Germany, is one of the most important submarine cables accessed by the "Five Eyes". Singapore, a former British colony in the Asia-Pacific region (blue dot), plays a vital role in intercepting Internet and telecommunications traffic heading from Australia/Japan to Europe, and vice versa. An intelligence-sharing agreement between Singapore and Australia allows the rest of the "Five Eyes" to gain access to SEA-ME-WE 3.^[94]

Right: TAT-14, a telecommunications cable linking Europe with the United States, was identified as one of few assets of "Critical Infrastructure and Key Resources" of the USA on foreign territory. In 2013, it was revealed that British officials "pressured a handful of telecommunications and Internet companies" to allow the British government to gain access to TAT-14.^[95]

According to the leaked documents, aside from the Five Eyes, most other Western countries have also participated in the NSA surveillance system and are sharing information with each other.^[96] In the documents the NSA lists "approved SIGINT partners" which are partner countries in addition to the Five Eyes. Glenn Greenwald said that the "NSA often maintains these partnerships by paying its partner to develop certain technologies and engage in surveillance, and can thus direct how the spying is carried out." These partner countries are divided into two groups, "Second Parties" and "Third Parties". The Second Parties are doing comprehensive cooperation with the NSA, and the Third Parties are doing focused cooperation.^{[97][98]} However, being a partner of the NSA does not automatically exempt a country from being targeted by the NSA itself. According to an internal NSA document leaked by Snowden, "We (the NSA) can, and often do, target the signals of most 3rd party foreign partners."^[99]



NSA lists "Approved SIGINT countries" which are divided into two groups by their cooperation level with the NSA.

- ☐ Second Parties
- ☐ Third Parties

Australia

The Australian Signals Directorate (ASD), formerly known as the Defence Signals Directorate (**DSD**), shares information on Australian citizens with the other members of the UKUSA Agreement. According to a 2008 Five Eyes document leaked by Snowden, data of Australian citizens shared with foreign countries include "bulk, unselected, unminimised metadata" as well as "medical, legal or religious information".^[102]

In close cooperation with other members of the Five Eyes community, the ASD runs secret surveillance facilities in many parts of Southeast Asia without the knowledge of Australian diplomats.^[103] In addition, the ASD cooperates with the Security and Intelligence Division (SID) of the Republic of Singapore in an international operation to intercept underwater telecommunications cables across the Eastern Hemisphere and the Pacific Ocean.^[104]

In March 2017 it was reported that, on advice from the Five Eyes intelligence alliance, more than 500 Iraqi and Syrian refugees, have been refused entry to Australia, in the last year.^[105]



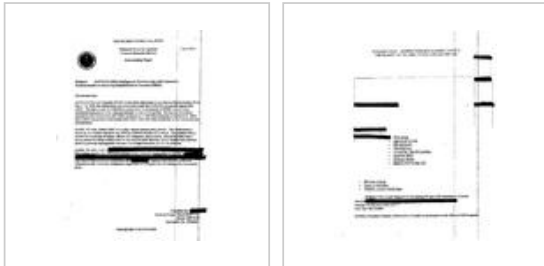
Pine Gap, near the Australian town of Alice Springs, is run by the CIA and it is part of the global surveillance program **ECHELON**.^{[100][101]}

Canada

The Communications Security Establishment Canada (**CSEC**) offers the NSA resources for advanced collection, processing, and analysis. It has set up covert sites at the request of NSA.^[106] The US-Canada SIGINT relationship dates back to a secret alliance formed during World War II, and was formalized in 1949 under the CANUSA Agreement.^[106]

On behalf of the NSA, the CSEC opened secret surveillance facilities in 20 countries around the world.^[107]

As well, the Communications Security Establishment Canada has been revealed, following the global surveillance disclosures to be engaging in surveillance on Wifi Hotspots of major Canadian Airports, collecting meta-data to use for engaging in surveillance on travelers, even days after their departure from said airports.^[108]



The NSA's relationship with Canada's CSEC NSA document on a mass surveillance operation with Canada's CSEC agency during the G8 and G20 summits in Toronto in 2010

Denmark

The Politiets Efterretningstjeneste (**PET**) of Denmark, a domestic intelligence agency, exchanges data with the NSA on a regular basis, as part of a secret agreement with the United States.^[109] Being one of the "9-Eyes" of the UKUSA Agreement, Denmark's relationship with the NSA is closer than the NSA's relationship with Germany, Sweden, Spain, Belgium or Italy.^[110]

France

The Directorate-General for External Security (**DGSE**) of France maintains a close relationship with both the NSA and the GCHQ after discussions for increased cooperation began in November 2006.^[111] By the early 2010s, the extent of cooperation in the joint interception of digital data by the DGSE and the NSA was noted to have increased dramatically.^{[111][112]}

In 2011, a formal memorandum for data exchange was signed by the DGSE and the NSA, which facilitated the transfer of millions of metadata records from the DGSE to the NSA.^[113] From December 2012 to 8 January 2013, over 70 million metadata records were handed over to the NSA by French intelligence agencies.^[113]

Germany

The Bundesnachrichtendienst (**BND**) of Germany systematically transfers metadata from German intelligence sources to the NSA. In December 2012 alone, the BND provided the NSA with 500 million metadata records.^[114] The NSA granted the Bundesnachrichtendienst access to X-Keyscore,^[115] in exchange for the German surveillance programs **Mira4** and **Veras**.^[114]

In early 2013, Hans-Georg Maaßen, President of the German domestic security agency Bundesamt für Verfassungsschutz (**BfV**), made several visits to the headquarters of the NSA. According to classified documents of the German government, Maaßen agreed to transfer all data records of persons monitored in Germany by the BfV via **XKeyscore** to the NSA.^[116] In addition, the BfV works very closely with eight other U.S. government agencies, including the CIA.^[117] Under **Project 6**, which is jointly operated by the CIA, BfV, and BND, a massive database containing personal information such as photos, license plate numbers, Internet search histories and telephone metadata was developed to gain a better understanding of the social relationships of presumed jihadists.^[118]

In 2012, the BfV handed over 864 data sets of personal information to the CIA, NSA and seven other U.S. intelligence agencies. In exchange, the BND received data from U.S. intelligence agencies on 1,830 occasions. The newly acquired data was handed over to the BfV and stored in a domestically accessible system known as **NADIS WN**.^[119]



The Dagger Complex in Darmstadt, Germany, is operated by the United States Army on behalf of the NSA. Similar to the NSA's Utah Data Center, the Dagger Complex is able to process, store, and decrypt millions of data pieces.^[120]

The Bad Aibling Station in Bavaria, Germany, was operated by the NSA until the early 2000s. It is currently run by the BND. As part of the global surveillance network **ECHELON**, it is the largest listening post outside Britain and the USA.^[121]

In 2013, the German news magazine *Der Spiegel* published an excerpt of an NSA document leaked by Snowden, showing that the BND used the NSA's **XKEYSCORE** to wiretap a German domestic target.

Israel

The Israeli SIGINT National Unit (**ISNU**) routinely receives raw, unfiltered data of U.S. citizens from the NSA. However, a secret NSA document leaked by Snowden revealed that U.S. government officials are explicitly exempted from such forms of data sharing with the ISNU.^[122] As stated in a memorandum detailing the rules of data sharing on U.S. citizens, the ISNU is obligated to:

Destroy upon recognition any communication contained in raw SIGINT provided by NSA that is either to or from an official of the U.S. government. "U.S. government officials" include officials of the Executive Branch (including White House, Cabinet Departments, and independent agencies); the U.S. House of Representatives and Senate (members and staff); and the U.S. Federal Court system (including, but not limited to, the Supreme Court).

— Memorandum of understanding between the NSA and Israel (circa 2009)

According to the undated memorandum, the ground rules for intelligence sharing between the NSA and the ISNU were laid out in March 2009.^[122] Under the data sharing agreement, the ISNU is allowed to retain the identities of U.S. citizens (excluding U.S. government officials) for up to a year.^[122]

Japan

In 2011, the NSA asked the Japanese government to intercept underwater fibre-optic cables carrying phone and Internet data in the Asia-Pacific region. However, the Japanese government refused to comply.^[123]

Libya

Under the reign of Muammar Gaddafi, the Libyan regime forged a partnership with Britain's secret service MI6 and the U.S. Central Intelligence Agency (CIA) to obtain information about Libyan dissidents living in the United States and Canada. In exchange, Gaddafi allowed the Western democracies to use Libya as a base for extraordinary renditions.^{[124][125][126][127][128]}

Netherlands

On 11 September 2013, *The Guardian* released a secret NSA document leaked by Snowden, which reveals how Israel's Unit 8200 (**ISNU**) was given raw, unfiltered data of U.S. citizens, as part of a secret agreement with the U.S. National Security Agency.^[122]



The Algemene Inlichtingen en Veiligheidsdienst (AIVD) of the Netherlands has been receiving and storing data of Internet users gathered by U.S. intelligence sources such as the NSA's **PRISM** surveillance program.^[129] During a meeting in February 2013, the AIVD and the MIVD briefed the NSA on their attempts to hack Internet forums and to collect the data of all users using a technology known as Computer Network Exploitation (CNE).^[130]



Summary of a meeting held in February 2013 between the NSA and the Dutch intelligence services AIVD and MIVD

Norway

The Norwegian Intelligence Service (NIS) has confirmed that data collected by the agency is "shared with the Americans".^[131] Kjell Grandhagen, head of Norwegian military intelligence told reporters at a news conference that "We share this information with partners, and partners share with us ... We are talking about huge amounts of traffic data".^[132]

In cooperation with the NSA, the NIS has gained access to Russian targets in the Kola Peninsula and other civilian targets. In general, the NIS provides information to the NSA about "Politicians", "Energy" and "Armament".^[133] A top secret memo of the NSA lists the following years as milestones of the **Norway-United States of America SIGNT agreement**, or NORUS Agreement:

- **1952** - Informal starting year of cooperation between the NIS and the NSA^[134]
- **1954** - Formalization of the NORUS Agreement^[134]
- **1963** - Extension of the agreement for coverage of foreign instrumentation signals intelligence (FISINT)^[134]
- **1970** - Extension of the agreement for coverage of electronic intelligence (ELINT)^[134]
- **1994** - Extension of the agreement for coverage of communications intelligence (COMINT)^[134]

The NSA perceives the NIS as one of its most reliable partners. Both agencies also cooperate to crack the encryption systems of mutual targets. According to the NSA, Norway has made no objections to its requests.^[134]

Singapore

The Defence Ministry of Singapore and its Security and Intelligence Division (SID) have been secretly intercepting much of the fibre optic cable traffic passing through the Asian continent. In close cooperation with the Australian Signals Directorate (ASD/DSD), Singapore's SID has been able to intercept SEA-ME-WE 3 (Southeast Asia-Middle East-Western Europe 3) as well as SEA-ME-WE 4 telecommunications cables.^[104] Access to these international telecommunications channels is facilitated by Singapore's government-owned operator, SingTel.^[104] Temasek Holdings, a multibillion-dollar sovereign wealth fund with a majority stake in SingTel, has maintained close relations with the country's intelligence agencies.^[104]

Information gathered by the Government of Singapore is transferred to the Government of Australia as part of an intelligence sharing agreement. This allows the "Five Eyes" to maintain a "stranglehold on communications across the Eastern Hemisphere".^[94]

Spain

In close cooperation with the Centro Nacional de Inteligencia (CNI), the NSA intercepted 60.5 million phone calls in Spain in a single month.^{[135][136]}

Sweden

The Försvarets radioanstalt (FRA) of Sweden (codenamed **Sardines**)^[137] has allowed the "**Five Eyes**" to access underwater cables in the Baltic Sea.^[137] On 5 December 2013, Sveriges Television (*Swedish Television*) revealed that the FRA has been conducting a clandestine surveillance operation targeting the internal politics of Russia. The operation was conducted on behalf of the NSA, which receives data handed over to it by the FRA.^{[138][139]}

According to documents leaked by Snowden, the FRA of Sweden has been granted access to the NSA's international surveillance program **XKeyscore**.^[140]



The NSA's relationship with Sweden's FRA under the UKUSA Agreement

Switzerland

The Federal Intelligence Service (NDB) of Switzerland exchanges information with the NSA regularly, on the basis of a secret agreement to circumvent domestic surveillance restrictions.^{[141][142]} In addition, the NSA has been granted access to Swiss surveillance facilities in Leuk (canton of Valais) and Herrenschwanden (canton of Bern), which are part of the Swiss surveillance program **Onyx**.^[141]

According to the NDB, the agency maintains working relationships with about 100 international organizations. However, the NDB has denied any form of cooperation with the NSA.^[143] Although the NSA does not have direct access to Switzerland's Onyx surveillance program, the Director of the NDB acknowledged that it is possible for other U.S. intelligence agencies to gain access to Switzerland's surveillance system.^[143]

United Kingdom

The British government allowed the NSA to store personal data of British citizens.^[144]

Under Project MINARET, anti-Vietnam War dissidents in the United States were jointly targeted by the GCHQ and the NSA.^{[145][146]}



RAF Menwith Hill, near Harrogate, North Yorkshire, is the biggest listening post outside the United States. It was used by U.S. military personnel to spy on Britons on behalf of MI5 and MI6.^[147]

United States

Central Intelligence Agency (CIA)

The CIA pays AT&T more than US\$10 million a year to gain access to international phone records, including those of U.S. citizens.^[148]

National Security Agency (NSA)

The NSA's Foreign Affairs Directorate interacts with foreign intelligence services and members of the Five Eyes to implement global surveillance.^[149]

Federal Bureau of Investigation (FBI)

The FBI acts as the liaison between U.S. intelligence agencies and Silicon Valley giants such as Microsoft.^[55]

Department of Homeland Security (DHS)

In the early 2010s, the DHS conducted a joint surveillance operation with the FBI to crack down on dissidents of the Occupy Wall Street protest movement.^{[150][151][152]}

Other law enforcement agencies

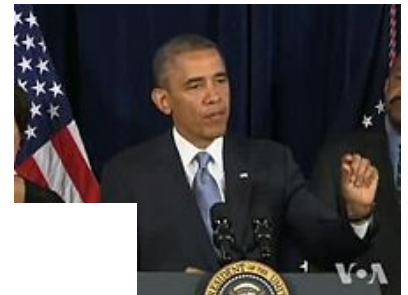
The NSA supplies domestic intercepts to the Drug Enforcement Administration (DEA), Internal Revenue Service (IRS), and other law enforcement agencies, who use intercepted data to initiate criminal investigations against US citizens. Federal agents are instructed to "recreate" the investigative trail in order to "cover up" where the information originated.^[44]

White House

Weeks after the September 11 attacks, U.S. President George W. Bush signed the Patriot Act to ensure no disruption in the government's ability to conduct global surveillance:

This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails, the Internet and cell phones.

— U.S. President George W. Bush on the implementation of the **Patriot Act** after the September 11 attacks^[153]



U.S. President Barack Obama emphasizing the importance of global surveillance to prevent terrorist attacks

The Patriot Act was extended by U.S. President Barack Obama in May 2011 to further extend the federal government's legal authority to conduct additional forms of surveillance such as roving wiretaps.^[154]

Commercial cooperation

Over 70 percent of the United States Intelligence Community's budget is earmarked for payment to private firms.^[155] According to *Forbes* magazine, the defense technology company Lockheed Martin is currently the USA's biggest defense contractor, and it is destined to be the NSA's most powerful commercial partner and biggest contractor in terms of dollar revenue.^[156]

AT&T

In a joint operation with the NSA, the American telecommunications corporation AT&T operates Room 641A in the SBC Communications building in San Francisco to spy on Internet traffic.^[157] The CIA pays AT&T more than US\$10 million a year to gain access to international phone records, including those of U.S. citizens.^[148]

Booz Allen Hamilton

Projects developed by Booz Allen Hamilton include the **Strategic Innovation Group** to identify terrorists through social media, on behalf of government agencies.^[158] During the fiscal year of 2013, Booz Allen Hamilton derived 99% of its income from the government, with the largest portion of its revenue coming from the U.S. Army.^[158] In 2013, Booz Allen Hamilton was hailed by Bloomberg Businessweek as "the World's Most Profitable Spy Organization".^[159]

British Telecommunications

British Telecommunications (code-named **Remedy**^[160]), a major supplier of telecommunications, granted Britain's intelligence agency GCHQ "unlimited access" to its network of undersea cables, according to documents leaked by Snowden.^[160]

Microsoft

The American multinational corporation **Microsoft** helped the NSA to circumvent software encryption safeguards. It also allowed the federal government to monitor web chats on the *Outlook.com* portal.^[55] In 2013, Microsoft worked with the FBI to allow the NSA to gain access to the company's cloud storage service *SkyDrive*.^[55]

Orange S.A.

The French telecommunications corporation **Orange S.A.** shares customer call data with the French intelligence agency DGSE, and the intercepted data is handed over to GCHQ.^[161]

RSA Security

RSA Security was paid US\$10 million by the NSA to introduce a cryptographic backdoor in its encryption products.^[162]

Stratfor

Strategic Forecasting, Inc., more commonly known as **Stratfor**, is a global intelligence company offering information to governments and private clients including Dow Chemical Company, Lockheed Martin, Northrop Grumman, Raytheon, the U.S. Department of Homeland Security, the U.S. Defense Intelligence Agency, and the U.S. Marine Corps.^[163]



French telecommunications corporation Orange S.A. shares customer call data with intelligence agencies.^[161]

Vodafone

The British telecommunications company **Vodafone** (code-named **Gerontic**^[160]) granted Britain's intelligence agency GCHQ "unlimited access" to its network of undersea cables, according to documents leaked by Snowden.^[160]

In-Q-Tel

In-Q-Tel, which receives more than US\$56 million a year in government support,^[164] is a venture capital firm that enables the CIA to invest in Silicon Valley.^[164]

Palantir Technologies

Palantir Technologies is a data mining corporation with close ties to the FBI, NSA and CIA.^{[165][166]}

Based in Palo Alto, California, the company developed a data collection and analytical program known as **Prism**.^{[167][168]}

In 2011, it was revealed that the company conducted surveillance on Glenn Greenwald.^{[169][170]}

Surveillance evasion

Several countries have evaded global surveillance by constructing secret bunker facilities deep below the Earth's surface.^[171]

North Korea

Despite North Korea being a priority target, the NSA's internal documents acknowledged that it did not know much about Kim Jong Un and his regime's intentions.^[80]

Iran

In October 2012, Iran's police chief Esmail Ahmadi Moghaddam alleged that Google is not a search engine but "a spying tool" for Western intelligence agencies.^[172] Six months later in April 2013, the country announced plans to introduce an "Islamic Google Earth" to evade global surveillance.^[173]

Libya

Libya evaded surveillance by building "hardened and buried" bunkers at least 40 feet below ground level.^[171]

Impact

The global surveillance disclosure has caused tension in the bilateral relations of the United States with several of its allies and economic partners as well as in its relationship with the European Union. On 12 August 2013, President Obama announced the creation of an "independent" panel of "outside experts" to review the NSA's surveillance programs. The panel is due to be established by the Director of National Intelligence, James R. Clapper, who will consult and provide assistance to them.^[174]

According to a survey undertaken by the human rights group PEN International, these disclosures have had a chilling effect on American writers. Fearing the risk of being targeted by government surveillance, 28% of PEN's American members have curbed their usage of social media, and 16% have self-censored themselves by avoiding controversial topics in their writings.^[175]



"Stop Watching Us" rally in Berlin, Germany, August 2014

See also

- 2013 Department of Justice investigations of reporters
- Terrorist Finance Tracking Program
- Top Secret America
- Global issue

References

- Webb, Maureen (2007). *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World* (1st ed.). San Francisco: City Lights Books. ISBN 0872864766.
- "Q&A: What you need to know about Echelon" (<http://news.bbc.co.uk/2/hi/sci/tech/1357513.stm>). BBC. 29 May 2001.
- Nabbali, Talitha; Perry, Mark (March 2004). "Going for the throat" (<http://www.sciencedirect.com/science/article/pii/S0267364904000184>). *Computer Law & Security Review*. **20** (2): 84–97. doi:10.1016/S0267-3649(04)00018-4 (<https://doi.org/10.1016%2FS0267-3649%2804%2900018-4>). "It wasn't until 1971 that the UKUSA allies began ECHELON"
- Zevenbergen, Bendert (3 December 2013). "Adventures in digital surveillance" (<https://link.springer.com/article/10.1007/s12290-013-0287-x>). *European View*. **12** (2): 223–233. doi:10.1007/s12290-013-0287-x (<https://doi.org/10.1007%2Fs12290-013-0287-x>). Retrieved 17 December 2013. "Snowden used the press to inform the world that a global surveillance state may be being built. This led to the beginning of a global political debate on digital communications surveillance."
- Ranger, Steve (24 March 2015). "The undercover war on your internet secrets: How online surveillance cracked our trust in the web" (<https://web.archive.org/web/20160612190952/http://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/>). TechRepublic. Archived from the original (<http://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/>) on 2016-06-12. Retrieved 2016-06-12.
- Laura Poitras; Marcel Rosenbach; Holger Stark. "Codename 'Apalachee': How America Spies on Europe and the UN" (<http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html>). *Der Spiegel*. p. 2. Retrieved August 26, 2013.
- MacAskill, Ewen; Davies, Nick; Hopkins, Nick; Borger, Julian; Ball, James (June 17, 2013). "GCHQ intercepted foreign politicians' communications at G20 summits" (<https://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits>). *The Guardian*. London.
- "Edward Snowden: US government has been hacking Hong Kong and China for years" (<http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china?page=all>). *South China Morning Post*. Retrieved September 9, 2013.
- Laura Poitras; Marcel Rosenbach; Fidelius Schmid; Holger Stark. "Attacks from America: NSA Spied on European Union Offices" (<http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html>). *Der Spiegel*. Retrieved September 9, 2013.

10. Staff (August 31, 2013). "Snowden Document: NSA Spied On Al Jazeera Communications" (<http://www.spiegel.de/international/world/nsa-spied-on-al-jazeera-communications-snowden-document-a-919681.html>). Retrieved August 31, 2013.
11. ROMERO, SIMON (9 September 2013). "N.S.A. Spied on Brazilian Oil Company, Report Says" (https://www.nytimes.com/2013/09/09/world/americas/nsa-spied-on-brazilian-oil-company-report-says.html?_r=0). *The New York Times*. Retrieved September 9, 2013.
12. "US bugged Merkel's phone from 2002 until 2013, report claims" (<https://www.bbc.co.uk/news/world-europe-24690055>). BBC. 27 October 2013. Retrieved October 27, 2013.
13. Ofer Aderet. "Snowden documents reveal U.S., British intelligence spied on former Prime Minister Olmert, Defense Minister Barak" (<http://www.haaretz.com/news/diplomacy-defense/1.564607>). *Haaretz*. Retrieved 20 December 2013.
14. James Ball; Nick Hopkins. "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief" (<https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner>). *The Guardian*. Retrieved 20 December 2013.
15. Michael Brissenden (18 Nov 2013). "Australia spied on Indonesian president Susilo Bambang Yudhoyono, leaked Edward Snowden documents reveal" (<http://www.abc.net.au/news/2013-11-18/australia-spied-on-indonesian-president-leaked-documents-reveal/5098860>). Australian Broadcasting Corporation. Retrieved 13 December 2013.
16. Ewen MacAskill and Lenore Taylor. "NSA: Australia and US used climate change conference to spy on Indonesia" (<https://www.theguardian.com/world/2013/nov/02/nsa-australia-bali-conference-spy-indonesia>). *The Guardian*. Retrieved 21 December 2013.
17. James Ball. "Xbox Live among game services targeted by US and UK spy agencies" (<https://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life>). *The Guardian*. Retrieved 25 December 2013.
18. "Pre-Emption - The Nsa And The Telecoms - Spying On The Home Front - FRONTLINE - PBS" (<https://www.pbs.org/wgbh/pages/frontline/homefront/preemption/telecoms.html>). *pbs.org*. Retrieved 8 March 2015.
19. Cohen, Martin. *No Holiday*. New York: Disinformation Company Ltd. ISBN 978-1-932857-29-0.
20. Peggy Becker (October 1999). DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION (http://bookshop.europa.eu/en/development-of-surveillance-technology-and-risk-of-abuse-of-economic-information-pbQASTOA132/downloads/QA-ST-OA-132-EN-N/QASTOA132ENN_002.pdf;pgid=y8dIS7GUWMdSR0EAIIMEUUsWb00002IUlfz2M;sid=w3lJEyGE1rNJH3CegDfXtEOhYbo1Q2zn3Qs=?FileName=QASTOA132ENN_002.pdf&SKU=QASTOA132ENN_PDF&CatalogueNumber=QA-ST-OA-132-EN-N) (Report). STOA, European Parliament. Retrieved 31 January 2014.
21. "Snowden has 'thousands' of damaging NSA documents, says Greenwald" (<http://tv.msnbc.com/2013/07/15/snowden-has-thousands-of-damaging-nsa-documents-says-greenwald/>). *MSNBC*. Retrieved 8 March 2015.
22. Glenn Greenwald; Ewen MacAskill (8 June 2013). "Boundless Informant: the NSA's secret tool to track global surveillance data" (<https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>). *The Guardian*. London. Retrieved 12 June 2013.
23. "Senators: Limit NSA snooping into US phone records" (<https://web.archive.org/web/20131029003314/http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records>). *Associated Press*. Archived from the original (<http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records>) on 29 October 2013. Retrieved 15 October 2013. ""Is it the goal of the NSA to collect the phone records of all Americans?" Udall asked at Thursday's hearing. "Yes, I believe it is in the nation's best interest to put all the phone records into a lockbox that we could search when the nation needs to do it. Yes," Alexander replied."
24. Siobhan Gorman. "Meltdowns Hobble NSA Data Center" (<https://www.wsj.com/news/articles/SB10001424052702304441404579119490744478398>). *The Wall Street Journal*. Retrieved 19 October 2013. "The Utah facility, one of the Pentagon's biggest U.S. construction projects, has become a symbol of the spy agency's surveillance prowess, which gained broad attention in the wake of leaks from NSA contractor Edward Snowden."
25. Shane Harris (August 22, 2012). "Who's Watching the N.S.A Watchers?" (<https://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html>). *The New York Times*. Retrieved 25 December 2013.
26. Duran-Sanchez, Mabel (10 August 2013). "Greenwald Testifies to Brazilian Senate about NSA Espionage Targeting Brazil and Latin America" (<http://www.cepr.net/index.php/blogs/the-americas-blog/greenwald-testifies-to-brazilian-senate-about-nsa-espionage-targeting-brazil-and-latin-america>). Retrieved 13 August 2013.
27. "Glenn Greenwald afirma que documentos dizem respeito à interesses comerciais do governo americano" (http://www.senado.gov.br/noticias/TV/default.asp?IND_ACESSO=S&cod_midia=269827&cod_video=267526). 6 August 2013. Retrieved 13 August 2013.
28. How Microsoft handed the NSA access to encrypted messages (<https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data>), *The Guardian*, 12 July 2013. Retrieved 13 July 2013.
29. Bridie Jabour in Sydney (12 July 2013). "Telstra signed deal that would have allowed US spying" (<https://www.theguardian.com/world/2013/jul/12/telstra-deal-america-government-spying>). *The Guardian*. London.
30. The first three days of revelations were: the FISC court order that Verizon provide bulk metadata to its customers to the NSA; presentation slides explaining the cooperation of nine US internet giants through the PRISM program; and the bulk collection of Chinese users' text messages, which coincided with Xi Jinping's visit to California to meet Barack Obama.
31. Shorrock, Tim (15 April 2013). "The Untold Story: Obama's Crackdown on Whistleblowers: The NSA Four reveal how a toxic mix of cronyism and fraud blinded the agency before 9/11" (<http://www.thenation.com/article/173521/obamas-crackdown-whistleblowers>). *The Nation*.
32. JAMES RISEN; ERIC LICHTBLAU (16 December 2005). "Bush Lets U.S. Spy on Callers Without Courts" (<https://www.nytimes.com/2005/12/16/politics/16program.html>). *The New York Times*.
33. Leslie Cauley (11 May 2006). "NSA has massive database of Americans' phone calls" (http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm). *USA Today*.

34. Poulsen, Kevin (6 March 2008). "Whistle-Blower: Feds Have a Backdoor Into Wireless Carrier — Congress Reacts" (<https://www.wired.com/threatlevel/2008/03/whistleblower-f/>). *Wired*. Retrieved 14 August 2013.
35. Maass, Peter (18 August 2013). "How Laura Poitras Helped Snowden Spill His Secrets" (<https://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html>). *The New York Times*.
36. Laura Poitras; Marcel Rosenbach; Holger Stark. "Ally and Target: US Intelligence Watches Germany Closely" (<http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html>). *Der Spiegel*. Retrieved August 13, 2013.
37. DeYoung, Karen (12 August 2013). "Colombia asks Kerry to explain NSA spying" (https://www.washingtonpost.com/politics/kerry-to-face-questions-on-nsa-spying-during-south-america-trip/2013/08/12/afdad47e-0382-11e3-88d6-d5795fab4637_story.html). *The Washington Post*. Retrieved August 13, 2013.
38. "Greenwald diz que espionagem dá vantagens comerciais e industriais aos Estados Unidos" (<http://www12.senado.gov.br/noticias/materias/2013/08/06/greenwald-diz-que-espionagem-da-vantagens-comerciais-e-industriais-aos-estados-unidos>) (in Portuguese). Federal Senate of Brazil. Retrieved August 13, 2013.
39. "Greenwald diz que EUA espionam para obter vantagens comerciais" (<http://www.dw.de/greenwald-diz-que-eua-espionam-para-obter-vantagens-comerciais/a-17002867>) (in Portuguese). Deutsche Welle. Retrieved August 13, 2013.
40. "NSA's activity in Latin America is 'collection of data on oil and military purchases from Venezuela, energy and narcotics from Mexico' – Greenwald" (http://voiceofrussia.com/news/2013_08_07/NSA-s-activity-in-Latin-America-is-collection-of-data-on-oil-and-military-purchases-from-Venezuela-energy-and-narcotics-from-Mexico-Greenwald-1337/). Voice of Russia. Retrieved August 13, 2013.
41. "Snowden: NSA's indiscriminate spying 'collapsing' - The Washington Post" (https://web.archive.org/web/20131217122329/http://www.washingtonpost.com/world/the_americas/report-snowden-would-help-brazil-if-given-asylum/2013/12/17/6ca6b7f8-66f0-11e3-997b-9213b17dac97_story.html). Archived from the original (https://www.washingtonpost.com/world/the_americas/report-snowden-would-help-brazil-if-given-asylum/2013/12/17/6ca6b7f8-66f0-11e3-997b-9213b17dac97_story.html) on 2013-12-17.
42. http://investigations.nbcnews.com/_news/2013/12/20/21975158-nsa-program-stopped-no-terror-attacks-says-white-house-panel-member
43. Finn, Peter (28 June 2013). "National Security" (https://www.washingtonpost.com/world/national-security/nsa-chief-says-surveillance-programs-helped-thwart-dozens-of-plots/2013/06/27/e97ab0a2-df70-11e2-963a-72d740e88c12_story.html). *The Washington Post*.
44. "Exclusive: U.S. directs agents to cover up program used to investigate Americans" (<https://www.reuters.com/article/2013/08/05-us-dea-sod-idUSBRE97409R20130805>). Reuters. 5 August 2013. Retrieved 14 August 2013.
45. "Senators: Limit NSA snooping into US phone records" (<https://web.archive.org/web/20131029003314/http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records>). *Associated Press*. Archived from the original (<http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records>) on 29 October 2013. Retrieved 15 October 2013.
46. John Miller. "NSA speaks out on Snowden, spying" (<http://www.cbsnews.com/news/nsa-speaks-out-on-snowden-spying/>). CBS News. Retrieved 17 December 2013. "What they are doing is collecting the phone records of more than 300 million Americans."
47. Greenwald, Glenn (31 July 2013). "XKeyscore: NSA tool collects 'nearly everything a user does on the internet' – XKeyscore Gives 'Widest-Reaching' Collection of Online Data – NSA Analysts Require No Prior Authorization for Searches – Sweeps Up Emails, Social Media Activity and Browsing History" (<https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>). *The Guardian*. Retrieved 1 August 2013.
48. Nakashima, Ellen (31 July 2013). "Newly declassified documents on phone records program released" (https://www.washingtonpost.com/world/national-security/governments-secret-order-to-verizon-to-be-unveiled-at-senate-hearing/2013/07/31/233fdd3a-f9cf-11e2-a369-d1954abcb7e3_story.html). *The Washington Post*. Retrieved 4 August 2013.
49. Charlie Savage; David E. Sanger (31 July 2013). "Senate Panel Presses N.S.A. on Phone Logs" (<https://www.nytimes.com/2013/08/01/us/nsa-surveillance.html?pagewanted=all&r=0>). *The New York Times*. Retrieved 4 August 2013.
50. Ball, James (25 October 2013). "Leaked memos reveal GCHQ efforts to keep mass surveillance secret" (<https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden>). *The Guardian*. Retrieved 25 October 2013.
51. Gellman, Barton; Poitras, Laura (6 June 2013). "US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program" (https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html). *The Washington Post*. Retrieved 15 June 2013.
52. "Documents on N.S.A. Efforts to Diagram Social Networks of U.S. Citizens" (<https://www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html>). *The New York Times*. September 28, 2013. Retrieved 17 December 2013.
53. James Risen; Laura Poitras (28 September 2013). "N.S.A. Gathers Data on Social Connections of U.S. Citizens" (https://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0&pagewanted=all). *The New York Times*. Retrieved 30 September 2013.
54. Barton Gellman; Ashkan Soltani (1 November 2013). "NSA collects millions of e-mail address books globally" (https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html). *The Washington Post*. Retrieved 20 December 2013.
55. Glenn Greenwald; Ewen MacAskill; Laura Poitras; Spencer Ackerman; Dominic Rushe. "Microsoft handed the NSA access to encrypted messages" (<https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data>). *The Guardian*. Retrieved 22 December 2013.

56. ["Follow the Money': NSA Spies on International Payments"](http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html) (<http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html>). *Der Spiegel*. Retrieved 23 October 2013.
57. Barton Gellman; Ashkan Soltani (4 December 2013). "NSA tracking cellphone locations worldwide, Snowden documents show" (https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html). *The Washington Post*. Retrieved 5 December 2013.
58. ["How the NSA is tracking people right now"](https://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/) (<https://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/>). *The Washington Post*. 4 December 2013. Retrieved 6 December 2013.
59. Ashkan Soltani; Matt DeLong (4 December 2013). ["FASCIA: The NSA's huge trove of location records"](https://apps.washingtonpost.com/g/page/world/what-is-fascia/637/) (<https://apps.washingtonpost.com/g/page/world/what-is-fascia/637/>). *The Washington Post*. Retrieved 6 December 2013.
60. ["How the NSA uses cellphone tracking to find and 'develop' targets"](https://www.washingtonpost.com/posttv/national/how-the-nsa-uses-cellphone-tracking-to-find-and-develop-targets/2013/12/04/d9114d52-5d1f-11e3-95c2-13623eb2b0e1_video.html) (https://www.washingtonpost.com/posttv/national/how-the-nsa-uses-cellphone-tracking-to-find-and-develop-targets/2013/12/04/d9114d52-5d1f-11e3-95c2-13623eb2b0e1_video.html). *The Washington Post*. 4 December 2013. Retrieved 6 December 2013.
61. ["Reporter explains NSA collection of cellphone data"](https://www.washingtonpost.com/posttv/politics/reporter-explains-nsa-collection-of-cellphone-data/2013/12/04/67b85252-5d26-11e3-95c2-13623eb2b0e1_video.html) (https://www.washingtonpost.com/posttv/politics/reporter-explains-nsa-collection-of-cellphone-data/2013/12/04/67b85252-5d26-11e3-95c2-13623eb2b0e1_video.html). *The Washington Post*. 4 December 2013. Retrieved 6 December 2013.
62. Peterson, Andrea (4 December 2013). ["The NSA says it 'obviously' can track locations without a warrant. That's not so obvious"](https://www.washingtonpost.com/blogs/the-switch/wp/2013/12/04/the-nsa-says-it-obviously-can-track-locations-without-a-warrant-that-s-not-so-obvious/) (<https://www.washingtonpost.com/blogs/the-switch/wp/2013/12/04/the-nsa-says-it-obviously-can-track-locations-without-a-warrant-that-s-not-so-obvious/>). *The Washington Post's The Switch*. Retrieved 6 December 2013.
63. Lee, Timothy (4 December 2013). ["The NSA could figure out how many Americans it's spying on. It just doesn't want to"](https://www.washingtonpost.com/blogs/the-switch/wp/2013/12/04/the-nsa-could-figure-out-how-many-americans-its-spying-on-it-just-doesnt-want-to/?tid=up_next) (https://www.washingtonpost.com/blogs/the-switch/wp/2013/12/04/the-nsa-could-figure-out-how-many-americans-its-spying-on-it-just-doesnt-want-to/?tid=up_next). *The Washington Post's The Switch*. Retrieved 6 December 2013.
64. Craig Timberg; Ashkan Soltani. ["By cracking cellphone code, NSA has capacity for decoding private conversations"](https://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html) (https://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html). *The Washington Post*. Retrieved 14 December 2013.
65. ["How the NSA pinpoints a mobile device"](https://apps.washingtonpost.com/g/page/world/how-the-nsa-pinpoints-a-mobile-device/645/#document/p2/a135576) (<https://apps.washingtonpost.com/g/page/world/how-the-nsa-pinpoints-a-mobile-device/645/#document/p2/a135576>). *The Washington Post*. Retrieved 14 December 2013.
66. Laura Poitras; Marcel Rosenbach; Holger Stark. ["iSpy: How the NSA Accesses Smartphone Data"](http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html) (<http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html>). *Der Spiegel*. Retrieved 9 September 2013.
67. Gellman, Barton; Soltani, Ashkan (30 October 2013). ["NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say"](https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html) (https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html). *The Washington Post*. Retrieved 31 October 2013.
68. Gellman, Barton; Soltani, Ashkan; Peterson, Andrea (4 November 2013). ["How we know the NSA had access to internal Google and Yahoo cloud data"](https://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/) (<https://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/>). *The Washington Post*. Retrieved 5 November 2013.
69. Barton Gellman; Craig Timberg; Steven Rich (4 October 2013). ["Secret NSA documents show campaign against Tor encrypted network"](https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html) (https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html). *The Washington Post*. Retrieved 19 November 2013.
70. Steven Rich; Matt DeLong (4 October 2013). ["NSA slideshow on 'The TOR problem'"](https://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/) (<https://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/>). *The Washington Post*. Retrieved 19 November 2013.
71. Lee, Timothy B. (4 October 2013). ["Everything you need to know about the NSA and Tor in one FAQ"](https://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/) (<https://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/>). *The Washington Post*. Retrieved 19 November 2013.
72. ["NSA report on the Tor encrypted network"](https://apps.washingtonpost.com/g/page/world/nsa-research-report-on-the-tor-encryption-program/501/) (<https://apps.washingtonpost.com/g/page/world/nsa-research-report-on-the-tor-encryption-program/501/>). *The Washington Post*. 4 October 2013. Retrieved 19 November 2013.
73. ["GCHQ report on 'MULLENIZE' program to 'stain' anonymous electronic traffic"](https://apps.washingtonpost.com/g/page/world/gchq-report-on-mullenize-program-to-stain-anonymous-electronic-traffic/502/) (<https://apps.washingtonpost.com/g/page/world/gchq-report-on-mullenize-program-to-stain-anonymous-electronic-traffic/502/>). *The Washington Post*. 4 October 2013. Retrieved 19 November 2013.
74. James Ball; Bruce Schneier; Glenn Greenwald (4 October 2013). ["NSA and GCHQ target Tor network that protects anonymity of web users"](https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption) (<https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption>). *The Guardian*. Retrieved 19 November 2013.
75. Schneier, Bruce (4 October 2013). ["Attacking Tor: how the NSA targets users' online anonymity"](https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity) (<https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>). *The Guardian*. Retrieved 19 November 2013.
76. ["Tor Stinks' presentation – read the full document"](https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document) (<https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>). *The Guardian*. 4 October 2013. Retrieved 19 November 2013.
77. ["Tor: 'The king of high-secure, low-latency anonymity'"](https://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity) (<https://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity>). *The Guardian*. 4 October 2013. Retrieved 19 November 2013.
78. Laura Poitras; Marcel Rosenbach; Holger Stark (17 November 2013). ["Royal Concierge': GCHQ Monitors Hotel Reservations to Track Diplomats"](http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html) (<http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html>). *Der Spiegel*. Retrieved 17 November 2013.

102. Ewen MacAskill; James Ball; Katharine Murphy. "Revealed: Australian spy agency offered to share data about ordinary citizens" (<https://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens>). *The Guardian*. Retrieved 3 December 2013.
103. Philip Dorling (31 October 2013). "Exposed: Australia's Asia spy network" (<http://www.smh.com.au/federal-politics/political-news/exposed-australias-asia-spy-network-20131030-2whia.html>). *The Sydney Morning Herald*. Retrieved 22 December 2013.
104. Philip Dorling. "Singapore, South Korea revealed as Five Eyes spying partners" (<http://www.smh.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html>). *The Sydney Morning Herald*. Retrieved 18 December 2013.
105. Benson, Simon (23 March 2017). "Security red flag for 500 refugees" (<http://www.theaustralian.com.au/national-affairs/immigration/security-red-flag-for-500-refugees-on-international-watchlist/news-story/129957e81c26c099045685818b56ceea>). *The Australian*. Retrieved 23 March 2017.
106. "NSA's Intelligence Relationship with Canada's Communications Security Establishment Canada (CSEC)" (<http://www.cbc.ca/news/2/pdf/nsa-canada-april32013.pdf>) (PDF). Canadian Broadcasting Corporation. Retrieved 22 December 2013.
107. Greg Weston; Glenn Greenwald; Ryan Gallagher. "Snowden document shows Canada set up spy posts for NSA" (<http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886>). Canadian Broadcasting Corporation. Retrieved 22 December 2013.
108. "CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents" (<http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>). *cbc.ca*. 31 January 2014. Retrieved 8 March 2015.
109. Justin Cremer. "Snowden leak confirms Denmark spying deal with US" (<http://cphpost.dk/news/snowden-leak-confirms-denmark-spying-deal-with-us.8185.html>). *The Copenhagen Post*. Retrieved 18 December 2013.
110. Justin Cremer. "Denmark is one of the NSA's '9-Eyes'" (<http://cphpost.dk/news/denmark-is-one-of-the-nsas-9-eyes.7611.html>). *The Copenhagen Post*. Retrieved 18 December 2013.
111. Jacques Follorou. "La France, précieux partenaire de l'espionnage de la NSA" (http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html) (in French). *Le Monde*. Retrieved 30 November 2013.
112. "Espionnage: les services secrets français précieux partenaires de la NSA américaine" (http://www.rfi.fr/ameriques/20131130-espionnage-services-secrets-francais-precieux-partenaires-nsa-americaine?ns_campaign=google_choix_redactions&ns_mchannel=editors_picks&ns_source=google_actuaite&ns_linkname=ameriques.20131130-espionnage-services-secrets-francais-precieux-partenaires-nsa-americaine&ns_fee=0) (in French). Radio France Internationale. Retrieved 30 November 2013.
113. Jacques Follorou (2013-10-30). "Surveillance : la DGSE a transmis des données à la NSA américaine" (http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html) (in French). *Le Monde*. Retrieved 30 December 2013.
114. "Überwachung: BND leitet massenhaft Metadaten an die NSA weiter" (<http://www.spiegel.de/netzwelt/netzpolitik/bnd-leitet-laut-spiegel-massenhaft-metadaten-an-die-nsa-weiter-a-914682.html>). *Der Spiegel* (in German). 3 August 2013. Retrieved 3 August 2013.
115. 'Prolific Partner': German Intelligence Used NSA Spy Program (<http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html>). *Der Spiegel*. Retrieved 21 July 2013.
116. "Verfassungsschutz beliefert NSA" (<http://www.sueddeutsche.de/politik/spionage-in-deutschland-verfassungsschutz-beliefert-nsa-1.1770672>) (in German). *Süddeutsche Zeitung*. Retrieved 14 September 2013. "Seit Juli 2013 testet der Verfassungsschutz die Späh- und Analysesoftware XKeyscore. Sollte der Geheimdienst das Programm im Regelbetrieb nutzen, hat sich das BfV verpflichtet, alle Erkenntnisse mit der NSA zu teilen. Das hatte der Präsident des Bundesamtes, Hans-Georg Maaßen, dem US-Dienst zugesichert. Im Januar und Mai war Maaßen zu Besuchen bei der NSA."
117. "Verfassungsschutz beliefert NSA" (<http://www.sueddeutsche.de/politik/spionage-in-deutschland-verfassungsschutz-beliefert-nsa-1.1770672>) (in German). *Süddeutsche Zeitung*. Retrieved 14 September 2013.
118. Matthias Gebauer; Hubert Gude; Veit Medick; Jörg Schindler; Fidelius Schmid. "CIA Worked With BND and BfV In Neuss on Secret Project" (<http://www.spiegel.de/international/germany/cia-worked-with-bnd-and-bfv-in-neuss-on-secret-project-a-921254.html>). *Der Spiegel*. Retrieved 20 December 2013.
119. Matthias Gebauer; Hubert Gude; Veit Medick; Jörg Schindler; Fidelius Schmid. "CIA Worked With BND and BfV In Neuss on Secret Project" (<http://www.spiegel.de/international/germany/cia-worked-with-bnd-and-bfv-in-neuss-on-secret-project-a-921254-2.html>). *Der Spiegel*. Retrieved 20 December 2013.
120. Christian Fuchs, John Goetz, Frederik Obermaier, Bastian Obermayer and Tanjev Schultz. "Frankfurt: An American Military-Intel Metropolis" (<http://international.sueddeutsche.de/post/67469252824/frankfurt-an-american-military-intel-metropolis>). *Süddeutsche Zeitung*. Retrieved 21 December 2013.
121. Shafir, Reinhard Wobst ; translated by Angelika (2007). *Cryptology unlocked*. Chichester: John Wiley & Sons. p. 5. ISBN 0470516194.
122. Glenn Greenwald; Laura Poitras; Ewen MacAskill (September 11, 2013). "NSA shares raw intelligence including Americans' data with Israel" (<https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>). *The Guardian*. Retrieved September 14, 2013.
123. "NSA asked Japan to tap regionwide fiber-optic cables in 2011" (<http://www.japantimes.co.jp/news/2013/10/27/world/nsa-asked-japan-to-tap-regionwide-fiber-optic-cables-in-2011/#.Um4Lf1NVO28>). *The Japan Times*. Retrieved 28 October 2013.
124. Wedeman, Ben (3 September 2011). "Documents shed light on CIA, Gadhafi spy ties" (<http://www.cnn.com/2011/WORLD/africa/09/03/libya.west.spies/>). *CNN*. Retrieved 3 September 2011.

125. "Libya: Gaddafi regime's US-UK spy links revealed" (<https://www.bbc.co.uk/news/world-africa-14774533>). BBC. 4 September 2011. Retrieved 20 December 2013.
126. Abigail Hauslohner (2 Sep 2011). "How Libya Seems to Have Helped the CIA with Rendition of Terrorism Suspects" (<http://content.time.com/time/world/article/0,8599,2091653,00.html>). *Time (magazine)*. Retrieved 20 December 2013.
127. "Files show MI6, CIA ties to Libya: reports" (<http://news.smh.com.au/breaking-news-world/files-show-mi6-cia-ties-to-libya-reports-20110904-1jrzy.html>). *The Sydney Morning Herald*. 4 September 2011. Retrieved 4 September 2011.
128. Spencer, Richard (3 September 2011). "Libya: secret dossier reveals Gaddafi's UK spy links" (<https://www.telegraph.co.uk/news/worldnews/africaandindianocean/libya/8739893/Libya-secret-dossier-reveals-Gaddafis-UK-spy-links.html>). *The Daily Telegraph*. London. Retrieved 3 September 2011.
129. Olmer, Bart. "Ook AIVD bespiedt internetter" (http://www.telegraaf.nl/binnenland/21638965/_Ook_AIVD_bespiedt_internetter_.html) (in Dutch). *De Telegraaf*. Retrieved 10 September 2013. "Niet alleen Amerikaanse inlichtingendiensten monitoren internetters wereldwijd. Ook Nederlandse geheime diensten krijgen informatie uit het omstreden surveillanceprogramma 'Prism'."
130. Steven Derix, Glenn Greenwald and Huib Modderkolk (30 November 2013). "Dutch intelligence agency AIVD hacks internet forums" (<http://www.nrc.nl/nieuws/2013/11/30/dutch-intelligence-agency-aivd-hacks-internet-fora/>). *NRC Handelsblad*. Retrieved 23 December 2013.
131. "Norway denies U.S. spying, said it shared intelligence with U.S." (<https://www.reuters.com/article/2013/11/19/us-norway-usa-snowden-idUSBRE9AI0D920131119>) Reuters. 19 November 2013. Retrieved 19 November 2013.
132. Kjetil Malkenes Hovland. "Norway Monitored Phone Traffic and Shared Data With NSA" (<https://www.wsj.com/news/articles/SB10001424052702303985504579207500439573552>). *The Wall Street Journal*. Retrieved 19 November 2013.
133. Arne Halvorsen; Anne Marte Blindheim; Harald S. Klungtveit; Kjetil Magne Sørenes; Tore Bergsaker; Gunnar Hultgreen. "Norway's secret surveillance of Russian politics for the NSA" (<http://www.dagbladet.no/2013/12/17/nyheter/samfunn/politikk/utenriks/overvakning/30877258/>). *Dagbladet*. Retrieved 18 December 2013.
134. "Snowden-dokumentene: Norge er NSAs drømmepartner" (<http://www.dagbladet.no/2013/12/18/nyheter/nsa/etterretningstjenesten/snowden/overvakning/30891164/>) (in Norwegian). *Dagbladet*. Retrieved 18 December 2013.
135. Paul Hamilos. "Spain colluded in NSA spying on its citizens, Spanish newspaper reports" (<https://www.theguardian.com/world/2013/oct/30/spain-colluded-nsa-spying-citizens-spanish-el-mundo-us>). *The Guardian*. Retrieved 22 December 2013.
136. Glenn Greenwald; Germán Aranda. "El CNI facilitó el espionaje masivo de EEUU a España" (<http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html>) (in Spanish). *El Mundo*. Retrieved 22 December 2013.
137. "Sverige deltog i NSA-övervakning" (http://www.svd.se/nyheter/inrikes/sverige-deltog-i-nsa-overvakning_8492260.svd) (in Swedish). *Svenska Dagbladet*. Retrieved 10 September 2013.
138. Glenn Greenwald, Ryan Gallagher, Filip Struwe and Anna H Svensson. "SVT avslöjar: FRA spionerar på Ryssland åt USA" (<https://web.archive.org/web/20131206130455/http://www.svt.se/nyheter/sverige/fra-spionerar-pa-ryssland-at-usa>) (in Swedish). *Sveriges Television*. Archived from the original (<http://www.svt.se/nyheter/sverige/fra-spionerar-pa-ryssland-at-usa>) on 6 December 2013. Retrieved 5 December 2013.
139. Filip Struwe, Glenn Greenwald, Ryan Gallagher, Sven Bergman, Joachim Dyfvermark and Fredrik Laurin. "Snowden files reveal Swedish-American surveillance of Russia" (<http://www.svt.se/ug/snowden-files-reveale-swedish-american-surveillance-of-russia>) (in Swedish). *Sveriges Television*. Retrieved 5 December 2013.
140. "Read the Snowden Documents From the NSA" (<http://www.svt.se/ug/read-the-snowden-documents-from-the-nsa>). *Sveriges Television*. Retrieved 12 December 2013.
141. "NDB und NSA kooperieren enger als bisher bekannt" (<http://www.handelszeitung.ch/politik/ndb-und-nsa-kooperieren-enger-als-bisher-bekannt-496751>) (in German). *Handelszeitung*. Retrieved 18 September 2013.
142. Christof Moser; Alan Cassidy. "Geheimdienst-Aufsicht will Kooperation des NDB mit der NSA prüfen" (<http://www.sonntagonline.ch/ressort/aktuell/3210/>) (in German). *Schweiz am Sonntag*. Retrieved 18 September 2013. "Die NSA hat sowohl mit der Schweiz wie Dänemark eine geheime Vereinbarung abgeschlossen, die den Austausch von Geheimdienstinformationen regelt. Die Vereinbarung berechtigt die NSA, eigene Schlüsselbegriffe in die Abhörssysteme beider Staaten einspeisen zu lassen. Im Tausch für damit gewonnene Erkenntnisse der schweizerischen und dänischen Auslandsaufklärung erhalten der NDB und der dänische Geheimdienst PET von der NSA Informationen, die sie im eigenen Land aufgrund gesetzlicher Schranken nicht selber sammeln dürfen. Das geheime Abkommen macht auch die Schweiz zu einem NSA-Horchposten."
143. Andy Müller. "Onyx: Gelangen Schweizer Abhördaten durch die Hintertür zur NSA?" (<http://www.srf.ch/news/schweiz/onyx-gelangen-schweizer-abhoerdaten-durch-die-hintertuer-zur-nsa>) (in German). *Schweizer Radio und Fernsehen*. Retrieved 18 December 2013.
144. Paul Mason (20 November 2013). "Documents show Blair government let US spy on Britons" (<http://www.channel4.com/news/nsa-edward-snowden-america-britain-tony-blair>). *Channel 4*. Retrieved 20 December 2013.
145. Christopher Hanson (13 August 1982). "British 'helped U.S. in spying on activists'" (<https://news.google.com/newspapers?id=t6FIAAAAIBAJ&sjid=VowNAAAAIBAJ&pg=1101,1439296&dq>). *The Vancouver Sun*. Retrieved 30 November 2013.
146. "'UK aided spy check'" (<https://news.google.com/newspapers?id=uwA-AAAAIBAJ&sjid=jkkMAAAAIBAJ&pg=5300,1649773&dq>). *Evening Times*. 13 August 1982. Retrieved 30 November 2013.
147. Chris Blackhurst; John Gilbert (22 September 1996). "US spy base 'taps UK phones for MI5'" (<https://www.independent.co.uk/news/uk/home-news/us-spy-base-taps-uk-phones-for-mi5-1364399.html>). London: *The Independent*. Retrieved 21 December 2013.
148. CHARLIE SAVAGE (7 November 2013). "C.I.A. Is Said to Pay AT&T for Call Data" (<https://www.nytimes.com/2013/11/07/us/cia-is-said-to-pay-att-for-call-data.html>). *The New York Times*. Retrieved 21 December 2013.

149. Marc Ambinder. "An Educated Guess About How the NSA Is Structured" (<https://www.theatlantic.com/technology/archive/2013/08/a-n-educated-guess-about-how-the-nsa-is-structured/278697/>). *The Atlantic*. Retrieved 21 December 2013.
150. Michael Hastings (28 February 2012). "Exclusive: Homeland Security Kept Tabs on Occupy Wall Street" (<https://www.rollingstone.com/politics/blogs/national-affairs/exclusive-homeland-security-kept-tabs-on-occupy-wall-street-20120228>). *Rolling Stone*. Retrieved 5 January 2014.
151. Naomi Wolf (29 December 2012). "Revealed: how the FBI coordinated the crackdown on Occupy" (<https://www.theguardian.com/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy>). *The Guardian*. Retrieved 5 January 2014.
152. MICHAEL S. SCHMIDT; COLIN MOYNIHAN (24 December 2012). "F.B.I. Counterterrorism Agents Monitored Occupy Movement, Records Show" (<https://www.nytimes.com/2012/12/25/nyregion/occupy-movement-was-investigated-by-fbi-counterterrorism-agents-records-show.html>). *The New York Times*. Retrieved 5 January 2014.
153. "Text: Bush Signs Anti-Terrorism Legislation" (https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushtext_102601.html). *The Washington Post*. 26 October 2001. Retrieved 21 December 2013.
154. Lisa Mascaro (Lisa Mascaro). "Patriot Act provisions extended just in time" (<http://articles.latimes.com/2011/may/27/nation/la-na-pat-riot-act-20110527>). *The Los Angeles Times*. Retrieved 22 December 2013. Check date values in: |date= (help)
155. Robert O'Harrow Jr., Dana Priest and Marjorie Censer (11 June 2013). "NSA leaks put focus on intelligence apparatus's reliance on outside contractors" (https://web.archive.org/web/20130928010248/http://articles.washingtonpost.com/2013-06-10/business/39873303_1_intelligence-agencies-intelligence-community-intelligence-analysts). *The Washington Post*. Archived from the original (https://articles.washingtonpost.com/2013-06-10/business/39873303_1_intelligence-agencies-intelligence-community-intelligence-analysts) on 28 September 2013. Retrieved 22 September 2013.
156. Loren Thompson (12 November 2013). "Lockheed Martin Emerging As Dominant Player In Federal Cybersecurity Market" (<https://www.forbes.com/sites/lorenthompson/2013/11/12/lockheed-martin-emerging-as-dominant-player-in-federal-cybersecurity-market/>). *Forbes*. Retrieved 22 December 2013.
157. "AT&T Whistle-Blower's Evidence" (<https://www.wired.com/science/discoveries/news/2006/05/70908>). *Wired*. 17 May 2006. Retrieved 27 February 2009.
158. Neil Irwin. "Seven facts about Booz Allen Hamilton" (<https://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/10/seven-facts-about-booz-allen-hamilton/>). *The Washington Post*. Retrieved 23 September 2013.
159. "Booz Allen, the World's Most Profitable Spy Organization" (<http://www.businessweek.com/articles/2013-06-20/booz-allen-the-world-s-most-profitable-spy-organization>). *Bloomberg Businessweek*. Retrieved 23 September 2013.
160. James Ball; Luke Harding; Juliette Garside. "BT and Vodafone among telecoms companies passing details to GCHQ" (<https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq>). *The Guardian*. Retrieved 22 December 2013.
161. Follorou, Jacques (20 March 2014). "Espionnage : comment Orange et les services secrets coopèrent" (http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html) (in French). *Le Monde*. Retrieved 22 March 2014.
162. Menn, Joseph (20 December 2013). "Exclusive: Secret contract tied NSA and security industry pioneer" (<https://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220>). San Francisco. *Reuters*. Retrieved 20 December 2013.
163. Pratap Chatterjee. "WikiLeaks' Stratfor dump lifts lid on intelligence-industrial complex" (<https://www.theguardian.com/commentisfree/cifamerica/2012/feb/28/wikileaks-intelligence-industrial-complex>). *The Guardian*. Retrieved 22 September 2013.
164. Steve Henn (16 July 2012). "In-Q-Tel: The CIA's Tax-Funded Player In Silicon Valley" (<https://www.npr.org/blogs/alltechconsidered/2012/07/16/156839153/in-q-tel-the-cias-tax-funded-player-in-silicon-valley>). *NPR*. Retrieved 5 January 2014.
165. "CIA-backed Palantir Technologies raises \$107.5 million" (<https://www.reuters.com/article/2013/12/11/venture-palantir-funding-idUSL1N0JQ1OE20131211>). *Reuters*. 11 December 2013. Retrieved 5 January 2014.
166. Andy Greenberg (2013-08-14). "How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut" (<https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/>). *Forbes*. Retrieved 5 January 2014.
167. "CIA-backed Palantir Technologies raises \$107.5 million" (<https://www.reuters.com/article/2013/12/11/venture-palantir-funding-idUSL1N0JQ1OE20131211>). *Reuters*. 11 December 2013. Retrieved 5 January 2014. "The Palo Alto., California-based start-up has drawn attention because of its Prism software product"
168. Ryan W. Neal (7 June 2013). "NSA Scandal: Is Palantir's Prism Powering PRISM?" (<http://www.ibtimes.com/nsa-scandal-palantir-prism-powering-prism-1296963>). *International Business Times*. Retrieved 5 January 2014.
169. Mike Masnick (10 Feb 2011). "Leaked HBGary Documents Show Plan To Spread Wikileaks Propaganda For BofA ... And 'Attack' Glenn Greenwald" (<http://www.techdirt.com/articles/20110209/22340513034/leaked-hbgary-documents-show-plan-to-spread-wikileaks-propaganda-bofa-attack-glenn-greenwald.shtml>). *Techdirt*. Retrieved 5 January 2014.
170. Mic Wright (21 September 2013). "Is 'Shadow' the creepiest startup ever? No, CIA investment Palantir still owns that crown" (<http://blogs.telegraph.co.uk/technology/micwright/100010629/is-shadow-the-creepiest-startup-ever-no-cia-investment-palantir-still-owns-that-crown/>). *The Daily Telegraph*. London. Retrieved 5 January 2014.
171. Narayan Lakshman (24 September 2013). "Secret bunkers, a challenge for U.S. intelligence" (<http://www.thehindu.com/news/international/world/secret-bunkers-a-challenge-for-us-intelligence/article5164833.ece>). Chennai, India: *The Hindu*. Retrieved 24 September 2013.
172. Elizabeth Flock (10 January 2012). "Google is 'a spying tool,' Iran police chief says" (https://www.washingtonpost.com/blogs/blogpost/post/google-is-a-spying-tool-iran-police-chief-says/2012/01/10/gIQA13b2nP_blog.html). *The Washington Post*. Retrieved 25 December 2013.

173. Saeed Kamali Dehghan (10 April 2013). "Iran plans 'Islamic Google Earth'" (<https://www.theguardian.com/world/2013/apr/10/iran-plans-islamic-google-earth>). *The Guardian*. Retrieved 25 December 2013.
174. Johnson, Luke (13 August 2013). "James Clapper, Director of National Intelligence Who Misled Congress, To Establish Surveillance Review Group" (http://www.huffingtonpost.com/2013/08/13/james-clapper_n_3748431.html). *Huffington Post*. Retrieved 13 August 2013.
175. Matt Sledge (13 November 2013). "NSA 'Chilling' Effect Feared By Writers" (http://www.huffingtonpost.com/2013/11/13/nsa-writers_n_4267716.html). *The Huffington Post*. Retrieved 14 November 2013.

Further reading

- "Global Surveillance" (<http://www.ub.uio.no/fag/informatikk-matematikk/informatikk/faglig/bibliografier/no21984.html>). An annotated and categorized "overview of the revelations following the leaks by the whistleblower Edward Snowden. There are also some links to comments and followups". By Oslo University Library.
- "The NSA Files" (<https://www.theguardian.com/world/the-nsa-files>). *The Guardian*. London. 8 June 2013.
- Politico Staff. "NSA leaks cause flood of political problems (<http://www.politico.com/story/2013/06/nsa-leaks-cause-flood-of-political-problems-92703.html>)." *Politico*. 13 June 2013.
- NSA inspector general report on email and internet data collection under Stellar Wind (<https://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection>) as provided by The Guardian on 27 June 2013.
- "Putin talks NSA, Syria, Iran, drones in exclusive RT interview (FULL VIDEO)" (<https://www.youtube.com/watch?v=33oIF-ggK5U>). "Russia Today". 12 June 2013.
- Ackerman, Spencer. "NSA warned to rein in surveillance as agency reveals even greater scope (<https://www.theguardian.com/world/2013/jul/17/nsa-surveillance-house-hearing>)." *The Guardian*. 17 July 2013.
- Ackerman, Spencer. "Slew of court challenges threaten NSA's relationship with tech firms (<https://www.theguardian.com/world/2013/jul/17/nsa-court-challenges-tech-firms>)." *The Guardian*. Wednesday, 17 July 2013.
- Ackerman, Spencer and Paul Lewis. "NSA amendment's narrow defeat spurs privacy advocates for surveillance fight (<https://www.theguardian.com/world/2013/jul/25/narrow-defeat-nsa-amendment-privacy-advocates>)." *The Guardian*. Thursday, 25 July 2013.
- Ackerman, Spencer and Dan Roberts. "US embassy closures used to bolster the case for NSA surveillance programs (<https://www.theguardian.com/world/2013/aug/05/us-embassy-closure-nsa-surveillance>)." *The Guardian*. Monday 5 August 2013.
- Two of the 'trips' (numbers 29 and 76) in the 2006 book, 'No Holiday', Cohen, Martin. *No Holiday*. New York: Disinformation Company Ltd. ISBN 978-1-932857-29-0. are investigating the NSA and its activities.
- Greenwald, Glenn. "Members of Congress denied access to basic information about NSA (<https://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access>)." *The Guardian*. Sunday 4 August 2013.
- Liu, Edward C. Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA) (<https://fas.org/srg/crs/intel/R44457.pdf>) Congressional Research Service, 13 April 2016.
- "Obama's former adviser ridicules statement that NSA doesn't spy on Americans (<http://rt.com/usa/us-obama-surveillance-snowden-296/>)." (Archive (<https://archive.is/20130810081243/http://rt.com/usa/us-obama-surveillance-snowden-296/>)) Russia Today. 9 August 2013.
- MacAskill, Ewen. "Justice Department fails in bid to delay landmark case on NSA collection (<https://www.theguardian.com/world/2013/jul/25/justice-department-case-nsa-collection>)." *The Guardian*. Thursday 25 July 2013.
- Rushe, Dominic. "Microsoft pushes Eric Holder to lift block on public information sharing (<https://www.theguardian.com/technology/2013/jul/16/microsoft-eric-holder-permission-information-national-security>)." *The Guardian*. Tuesday 16 July 2013.
- Perez, Evan. "Documents shed light on U.S. surveillance programs (<http://www.cnn.com/2013/08/09/politics/nsa-documents-scope/index.html>)." (Archive (<https://archive.is/20130810061150/http://edition.cnn.com/2013/08/09/politics/nsa-documents-scope/index.html>)) CNN. 9 August 2013.
- Gellman, Barton. "NSA broke privacy rules thousands of times per year, audit finds (https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html)." *Washington Post*. Thursday 15 August 2013.
- Roberts, Dan and Robert Booth. "NSA defenders: embassy closures followed pre-9/11 levels of 'chatter' (<https://www.theguardian.com/world/2013/aug/04/nsa-us-embassy-closures-terrorist-threat>)." *The Guardian*. Sunday 4 August 2013.
- Greenwald, Glenn. "The crux of the NSA story in one phrase: 'collect it all' (<https://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all>)." *The Guardian*. Monday 15 July 2013.
- Sanchez, Julian. "Five things Snowden leaks revealed about NSA's original warrantless wiretaps (<https://arstechnica.com/tech-policy/2013/07/5-things-snowden-leaks-revealed-about-nsas-original-warrantless-wiretaps/>)." *Ars Technica*. 9 July 2013.
- Forero, Juan. "Paper reveals NSA ops in Latin America (https://www.washingtonpost.com/world/the-americas/paper-reveals-nsa-ops-in-latin-america/2013/07/09/eff0cc7e-e8e3-11e2-818e-aa29e855f3ab_story.html)." *Washington Post*. 9 July 2013.
- Jabour, Bridie. "Telstra signed deal that would have allowed US spying (<https://www.theguardian.com/world/2013/jul/12/telstra-deal-america-government-spying>)." *The Guardian*. Friday 12 July 2013.
- Ackerman, Spencer. "White House stays silent on renewal of NSA data collection order (<https://www.theguardian.com/world/2013/jul/18/white-house-silent-renewal-nsa-court-order#start-of-comments>)." *The Guardian*. Thursday 18 July 2013.
- Naughton, John. "Edward Snowden's not the story. The fate of the internet is (<https://www.theguardian.com/technology/2013/jul/28/edward-snowden-death-of-internet>)." *The Guardian*. 28 July 2013.
- Adams, Becket. "MAD MAGAZINE USES ICONIC CHARACTERS TO HIT OBAMA OVER GOV'T SURVEILLANCE (<http://www.theblaze.com/stories/2013/08/08/mad-magazine-uses-iconic-characters-to-hit-obama-over-govt-surveillance/>)." *The Blaze*. 8 August 2013.
- Howerton, Jason. "HERE IS THE PRO-NSA SURVEILLANCE ARGUMENT (<http://www.theblaze.com/stories/2013/06/10/here-is-the-pro-nsa-surveillance-argument>)." *The Blaze*. 10 June 2013.
- "Edward Snowden NSA files: secret surveillance and our revelations so far – Leaked National Security Agency documents have led to several hundred Guardian stories on electronic privacy and the state (<https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations>)" by *The Guardian's* James Ball on 21 August 2013

- 2013-07-29 Letter of FISA Court president Reggie B. Walton to the Chairman of the U.S. Senate Judiciary Committee Patrick J. Leahy about certain operations of the FISA Court (<http://www.leahy.senate.gov/download/honorable-patrick-j-leahy>); among other things the process of accepting, modifying and/or rejecting surveillance measures proposed by the U.S. government, the interaction between the FISA Court and the U.S. government, the appearance of non-governmental parties before the court and the process used by the Court to consider and resolve any instances where the government entities notifies the court of compliance concerns with any of the FISA authorities.
 - "The Spy Files" (<https://wikileaks.org/the-spyfiles.html>). WikiLeaks. 1 December 2011. A collection of documents relating to surveillance.
 - "The Spy Files" (<https://wikileaks.org/spyfiles/list/releasedate/2011-12-08.html>). WikiLeaks. 8 December 2011. Part 2 of the above.
 - "Spy Files 3" (<https://wikileaks.org/spyfiles3.html>). WikiLeaks. 4 September 2013. Part 3 of the above.
 - "Veja os documentos ultrassecretos que comprovam espionagem a Dilma" (<http://g1.globo.com/fantastico/noticia/2013/09/veja-os-d-ocmentos-ultrassecretos-que-comprovam-espionagem-dilma.html>) (in Portuguese). 2 September 2013. Retrieved 4 September 2013. Documents relating to the surveillance against Dilma Rousseff and Enrique Peña Nieto
 - NSA surveillance: A guide to staying secure - The NSA has huge capabilities – and if it wants in to your computer, it's in. With that in mind, here are five ways to stay safe (<https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>) by *The Guardian's* Bruce Schneier on 5 September 2013.
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Global_surveillance&oldid=881787227"

This page was last edited on 4 February 2019, at 20:31 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.