

Global surveillance disclosures (2013–present)

From Wikipedia, the free encyclopedia

Ongoing news reports in the international media have revealed operational details about the U.S. National Security Agency (NSA) and its international partners' **global surveillance**^[1] of foreign nationals and U.S. citizens. The reports emanate from a cache of top secret documents leaked by ex-NSA contractor Edward Snowden. In June 2013, the first of Snowden's documents were published simultaneously by *The Washington Post* and *The Guardian*, attracting considerable public attention.^[2] The disclosure continued throughout the entire year of 2013, and a significant portion of the full cache of the estimated 1.7 million documents^[3] was later obtained and published by many other media outlets worldwide, most notably *The New York Times* (USA), *Der Spiegel* (Germany), Australian Broadcasting Corporation (Australia), *O Globo* (Brazil), the Canadian Broadcasting Corporation (Canada), *Le Monde* (France), *L'espresso* (Italy), *NRC Handelsblad* (the Netherlands), *Dagbladet* (Norway), *El País* (Spain), and Sveriges Television (Sweden).^[4]

In summary, these media reports have shed light on the implications of several secret treaties signed by members of the UKUSA Agreement in their efforts to implement global surveillance. For example, *Der Spiegel* revealed how the German Bundesnachrichtendienst (BND) transfers "massive amounts of intercepted data to the NSA",^[5] while Sveriges Television revealed that the Försvarets radioanstalt (FRA) of Sweden is continuously providing the NSA with intercepted data gathered from telecom cables, under a secret treaty signed in 1954 for bilateral cooperation on surveillance.^[6] Other security and intelligence agencies involved in the practice of global surveillance include those in Australia (ASD), Britain (GCHQ), Canada (CSEC), Denmark (PET), France (DGSE), Germany (BND), Italy (AISE), the Netherlands (AIVD), Norway (NIS), Spain (CNI), Switzerland (NDB), as well as Israel (ISNU), which receives raw, unfiltered data of U.S. citizens that is shared by the NSA.^{[7][8][9][10][11][12][13][14]}

The disclosure provided impetus for the creation of social movements against mass surveillance, such as Restore the Fourth, and actions like Stop Watching Us and The Day We Fight Back. Domestic spying programs in countries such as France, the UK, and India have also been exposed. On the legal front, the Electronic Frontier Foundation joined a coalition of diverse groups filing suit against the NSA. Several human rights organizations have urged the Obama administration not to prosecute, but protect, "whistleblower Snowden": Amnesty International, Human Rights Watch, Transparency International, and the Index on Censorship, *inter alia*.^{[15][16][17][18]}

On June 14, 2013, United States prosecutors charged Edward Snowden with espionage and theft of government property.^[19] In late July 2013, he was granted asylum by the Russian government,^[20] contributing to a deterioration of Russia–United States relations.^{[21][22]} On August 6, 2013, President Obama made a public appearance on national television where he reassured Americans that "We don't have a domestic spying program" and "There is no spying on Americans".^[23] Towards the end of October 2013, the British Prime Minister David Cameron warned *The Guardian* not to publish any more leaks, or it will receive a DA-Notice.^[24] Currently, a criminal investigation of the disclosure is being undertaken by Britain's Metropolitan Police Service.^[25] In December 2013, *The Guardian* editor Alan Rusbridger said: "We have published I think 26 documents so far out of the 58,000 we've seen."^[26]

The extent to which the media reports have responsibly informed the public is disputed. In January 2014 U.S. President Barack Obama said that "the sensational way in which these disclosures have come out has often

shed more heat than light"^[27] and critics such as Sean Wilentz have noted that many of the Snowden documents released do not concern domestic surveillance.^[28]

Contents

- 1 Overview
 - 1.1 Global surveillance
 - 1.2 Historical context
- 2 Timeline
 - 2.1 2013
 - 2.1.1 January–May
 - 2.1.2 June
 - 2.1.3 July
 - 2.1.4 August
 - 2.1.5 September
 - 2.1.6 October
 - 2.1.7 November
 - 2.1.8 December
 - 2.2 2014
 - 2.2.1 January
- 3 Aftermath
 - 3.1 Reactions of political leaders
 - 3.2 Review of intelligence agencies
 - 3.3 Criticism
- 4 Gallery
- 5 Exceptionally Controlled Information
- 6 Comparison with previous leaks
- 7 See also
- 8 References
- 9 External links

Overview

Barton Gellman, a Pulitzer Prize-winning journalist who led *The Washington Post*'s coverage of Snowden's disclosures, summarized the leaks as follows:

"Taken together, the revelations have brought to light a **global surveillance** system that cast off many of its historical restraints after the attacks of Sept. 11, 2001. Secret legal authorities empowered the NSA to sweep in the telephone, Internet and location records of whole populations."

















—*The Washington Post*^[29]

The disclosure revealed specific details of the NSA's close cooperation with U.S. federal agencies such as the Federal Bureau of Investigation (FBI)^{[30][31]} and the Central Intelligence Agency (CIA)^{[32][33]} in addition to

the agency's previously undisclosed financial payments to numerous commercial partners and telecommunications companies,^{[34][35][36]} as well as its previously undisclosed relationships with international partners such as Britain,^{[37][38]} France^{[12][39]} Germany,^{[5][40]} and its secret treaties with foreign governments that were recently established for sharing intercepted data of each other's citizens.^{[7][41][42][43]} The disclosures were made public over the course of several months since June 2013 by the press in several nations from the trove leaked by the former N.S.A. contractor Edward J. Snowden.^[44]

Global surveillance

Main article: Global surveillance

Global surveillance programs		
Program	International contributors and/or partners	Commercial partners
 PRISM	<ul style="list-style-type: none">  Australian Signals Directorate (ASD/DSD) of Australia^[45]  Government Communications Headquarters (GCHQ) of Great Britain^[46]  Algemene Inlichtingen en Veiligheidsdienst (AIVD) of the Netherlands^[47] 	<ul style="list-style-type: none"> Microsoft^{[30][48][49]}
 XKeyscore	<ul style="list-style-type: none">  Bundesnachrichtendienst (BND) of Germany^{[5][50]}  Bundesamt für Verfassungsschutz (BfV) of Germany^{[5][50]}  Försvarets radioanstalt (FRA) of Sweden^{[51][52]} 	
 Tempora	<ul style="list-style-type: none">  National Security Agency (NSA)^{[53][54]} 	<ul style="list-style-type: none"> British Telecommunications (codenamed "Remedy")^[55] Interoute (codenamed "Streetcar")^[55] Level 3 (codenamed "Little")^[55] Global Crossing (codenamed "Pinnage")^[55] Verizon Business (codenamed "Dacron")^[55] Viatel (codenamed "Vitreous")^[55] Vodafone Cable (codenamed "Gerontic")^[55]
 Muscular	<ul style="list-style-type: none">  NSA^[56] 	
 Project 6	<ul style="list-style-type: none">  Central Intelligence Agency (CIA)^[57] 	
Stateroom	<ul style="list-style-type: none">  DSD^{[58][59]}  Communications Security 	

	<div>Establishment Canada (CSEC)^{[59][60]}</div> <div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div>GCHQ^{[59][61]}</div></div> <div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div>Special Collection Service (SCS)^{[59][61][62]}</div></div>	
Lustre	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div>NSA^{[63][64]}</div></div> <div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div>Direction Générale de la Sécurité Extérieure (DGSE) of France^{[63][64]}</div></div>	

Last updated: December 2013

Historical context

Main article: Global surveillance disclosures (1970–2013)

In the 1970s, NSA analyst Perry Fellwock (under the pseudonym "Winslow Peck") revealed the existence of the UKUSA Agreement,^[65] which forms the basis of the **ECHELON** network, whose existence was revealed in 1988 by Lockheed employee Margaret Newsham.^[66] Months before the September 11 attacks and during its aftermath, further details of the global surveillance apparatus were provided by ex-MI5 official David Shayler,^[67] followed by James Bamford in 2001,^[68] William Binney and colleagues in 2002,^[69] Katharine Gun in 2003,^[70] Clare Short in 2004,^[71] journalists Eric Lichtblau and James Risen in 2005,^[72] Leslie Cauley of *USA Today* in 2006,^[73] Mark Klein in 2006,^[74] Russ Tice in 2006,^[75] Thomas Andrews Drake in 2010,^[76] Julian Assange and Chelsea Manning in 2011,^[77] and Michael Hastings in 2012.^[78]

Timeline

2012

In April 2012, Edward Snowden began downloading sensitive NSA material while working for the American computer corporation Dell.^[80] By the end of the year, Snowden had made his first contact with journalist Glenn Greenwald of *The Guardian*.^[81]

2013

January–May

In January 2013, Snowden contacted documentary filmmaker Laura Poitras.^[82] In March 2013, Snowden took up a new job at Booz Allen Hamilton in Hawaii, specifically to gain access to additional top-secret documents that could be leaked.^[80] In April 2013, Poitras asked Greenwald to meet her in New York City.^[81] In May 2013, Snowden was permitted temporary leave from his position at the NSA in Hawaii, on the pretext of receiving treatment for his epilepsy.^[83] Towards the end of



May, Snowden flew to Hong Kong.^[84]

June

After the U.S.-based editor of *The Guardian* held several meetings in New York City, it was decided that Greenwald, Poitras and the Guardian's defence and intelligence correspondent Ewen MacAskill would fly to Hong Kong to meet Snowden. On June 5, in the first media report based on the leaked material,^[85] *the Guardian* exposed a top secret court order showing that the NSA had collected phone records from over 120 million Verizon subscribers.^[86] Under the order, the numbers of both parties on a call, as well as the location data, unique identifiers, time of call, and duration of call were handed over to the FBI, which turned over the records to the NSA.^[86]

On June 6, 2013, the second media disclosure was published simultaneously by *The Guardian* and *The Washington Post*.^{[79][87]}

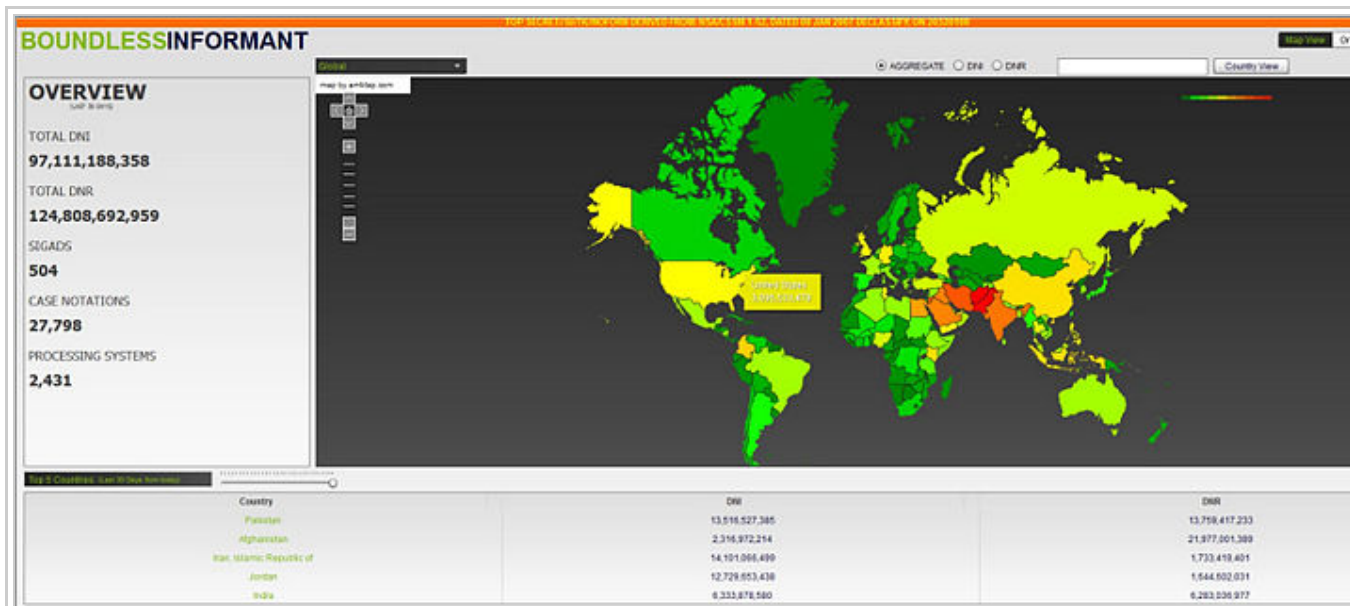
Documents provided by Snowden to *Der Spiegel* revealed how the NSA spied on various diplomatic missions of the European Union (EU) including the EU's delegation to the United States in Washington D.C., the EU's delegation to the United Nations in New York, and the Council of the European Union in Brussels, as well as the United Nations Headquarters in New York.^{[88][89]} During specific episodes within a four-year period, the NSA hacked several Chinese mobile-phone companies,^[90] the Chinese University of Hong Kong and Tsinghua University in Beijing,^[91] and the Asian fiber-optic network operator Pacnet.^[92] Only Australia, Canada, New Zealand and the UK are explicitly exempted from NSA attacks, whose main target in the EU is Germany.^[93] A method of bugging encrypted fax machines used at an EU embassy is codenamed Dropmire.^[94]

During the 2009 G-20 London summit, the British intelligence agency Government Communications Headquarters (**GCHQ**) intercepted the communications of foreign diplomats.^[95] In addition, the GCHQ has been intercepting and storing mass quantities of fiber-optic traffic via **Tempora**.^[96] Two principal components of Tempora are called "Mastering the Internet" (MTI) and "Global Telecoms Exploitation".^[97] The data is preserved for three days while metadata is kept for thirty days.^[98] Data collected by the GCHQ under Tempora is shared with the National Security Agency (NSA) of the United States.^[97]

From 2001 to 2011, the NSA collected vast amounts of metadata records detailing the email and internet usage of Americans via **Stellar Wind**,^[99] which was later terminated due to operational and resource constraints. It was subsequently replaced by newer surveillance programs such as **ShellTrumpet**, which "*processed its one trillionth metadata record*" by the end of December 2012.^[100]

According to the **Boundless Informant**, over 97 billion pieces of intelligence were collected over a 30-day period ending in March 2013. Out of all 97 billion sets of information, about 3 billion data sets originated from U.S. computer networks^[101] and around 500 million metadata records were collected from German networks.^[102]

Several weeks later, it was revealed that the Bundesnachrichtendienst (**BND**) of Germany transfers massive amounts of metadata records to the NSA.^[103]



On June 11, 2013, *The Guardian* published a snapshot of the NSA's global map of electronic data collection for the month of March 2013. Known as the **Boundless Informant**, the program is used by the NSA to track the amount of data being analyzed over a specific period of time. The color scheme ranges from green (least subjected to surveillance) through yellow and orange to red (most surveillance). Outside the Middle East, only China, Germany, India, Kenya, and the United States are colored orange or yellow

July

According to the Brazilian newspaper *O Globo*, the NSA spied on millions of emails and calls of Brazilian citizens,^{[104][105]} while Australia and New Zealand have been involved in the joint operation of the NSA's global analytical system **XKeyscore**.^{[106][107]} Among the numerous allied facilities contributing to XKeyscore are four installations in Australia and one in New Zealand:

- Pine Gap near Alice Springs, Australia, which is partly operated by the U.S. Central Intelligence Agency (CIA)^[107]
- The Shoal Bay Receiving Station near Darwin, Australia, is operated by the Australian Signals Directorate (ASD)^[107]
- The Australian Defence Satellite Communications Station near Geraldton, Australia, is operated by the ASD^[107]
- HMAS Harman outside Canberra, Australia, is operated by the ASD^[107]
- Waihopai Station near Blenheim, New Zealand, is operated by New Zealand's Government Communications Security Bureau (GCSB)^[107]

According to Edward Snowden, the NSA has established secret intelligence partnerships with many Western governments.^[107] The Foreign Affairs Directorate (FAD) of the NSA is responsible for these partnerships, which, according to Snowden, are organized such that foreign governments can "insulate their political leaders" from public outrage in the event that these global surveillance partnerships are leaked.^[108]

In an interview published by *Der Spiegel*, Snowden accused the NSA of being "in bed together with the

Germans".^[109] The NSA granted the German intelligence agencies BND (foreign intelligence) and BfV (domestic intelligence) access to its controversial **XKeyscore** system.^[110] In return, the BND turned over copies of two systems named **Mira4** and **Veras**, reported to exceed the NSA's SIGINT capabilities in certain areas.^[5] Every day, massive amounts of metadata records are collected by the BND and transferred to the NSA via the Bad Aibling Station near Munich, Germany.^[5] In December 2012 alone, the BND handed over 500 million metadata records to the NSA.^{[111][112]}

In a document dated January 2013, the NSA acknowledged the efforts of the BND to undermine privacy laws:

"The BND has been working to influence the German government to relax interpretation of the privacy laws to provide greater opportunities of intelligence sharing"^[112]

According to an NSA document dated April 2013, Germany has now become the NSA's "most prolific partner".^[112] Under a section of a separate document leaked by Snowden titled "Success Stories", the NSA acknowledged the efforts of the German government to expand the BND's international data sharing with partners:

"The German government modifies its interpretation of the G-10 privacy law ... to afford the BND more flexibility in sharing protected information with foreign partners."^[50]

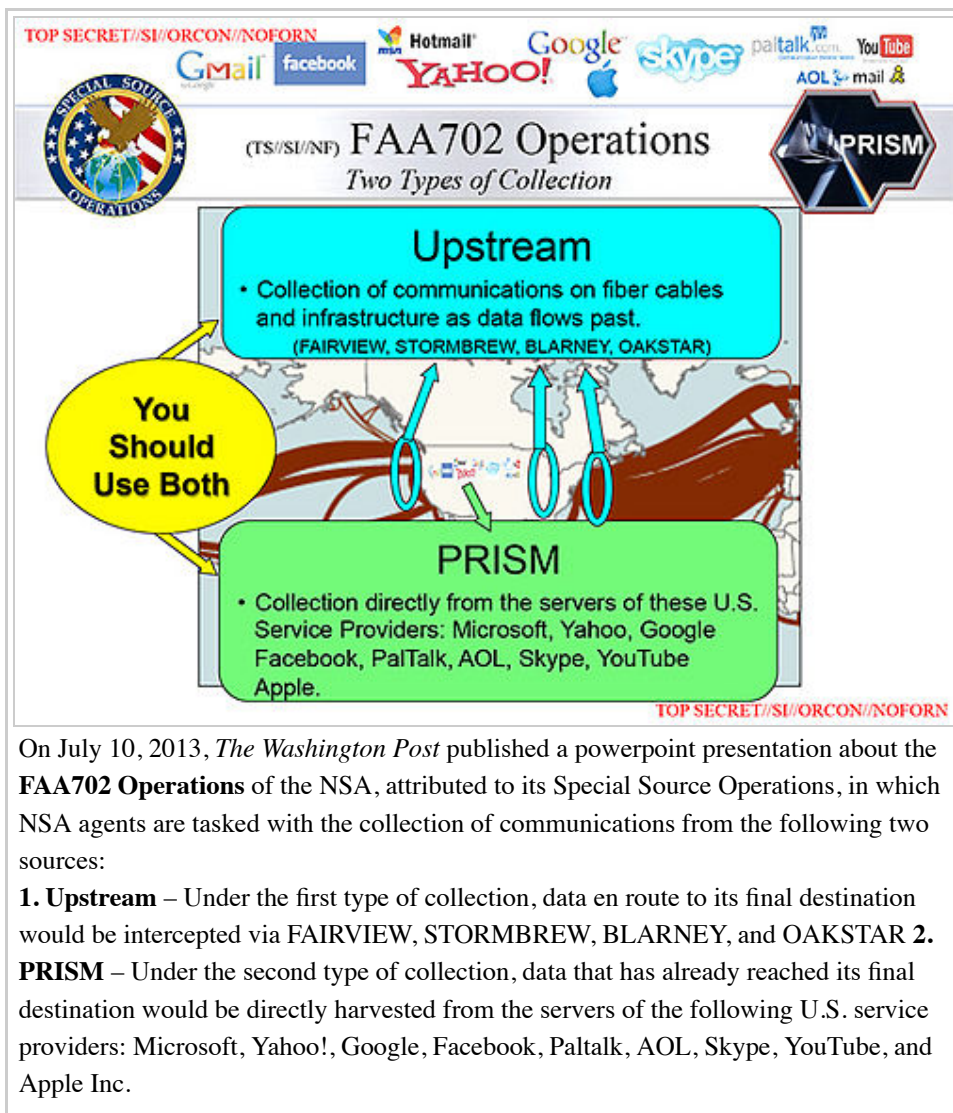
In addition, the German government was well aware of the PRISM surveillance program long before Edward Snowden made details public. According to Angela Merkel's spokesman Steffen Seibert, there are two separate PRISM programs - one is used by the NSA and the other is used by NATO forces in Afghanistan.^[113] Both surveillance programs are "not identical".^[113]

The Guardian revealed further details of the NSA's **XKeyscore** tool, which allows government analysts to search through vast databases containing emails, online chats and the browsing histories of millions of individuals without prior authorization.^{[114][115][116]} Microsoft "developed a surveillance capability to deal" with the interception of encrypted chats on Outlook.com, within five months after the service went into testing. NSA had access to Outlook.com emails because "Prism collects this data prior to encryption."^[48]

In addition, Microsoft worked with the FBI to enable the NSA to gain access to its cloud storage service SkyDrive. An internal NSA document dating from 3 August 2012 described the PRISM surveillance program as a "team sport".^[48]

Even if there is no reason to suspect U.S. citizens of wrongdoing, the CIA's National Counterterrorism Center is allowed to examine federal government files for possible criminal behavior. Previously the NTC was barred to do so, unless a person was a terror suspect or related to an investigation.^[117]

Snowden also confirmed that Stuxnet was cooperatively developed by the United States and Israel.^[118] In a report unrelated to Edward Snowden, the French newspaper *Le Monde* revealed that France's DGSE was also undertaking mass surveillance, which it described as "illegal and outside any serious control".^{[119][120]}



August

Documents leaked by Edward Snowden that were jointly disclosed by *Süddeutsche Zeitung* (SZ) and *Norddeutscher Rundfunk* revealed that several telecom operators have played a key role in helping the British intelligence agency Government Communications Headquarters (GCHQ) tap into worldwide fiber-optic communications. The telecom operators are:

- Verizon Business (codenamed "**Dacron**")^{[55][121]}
- British Telecommunications (codenamed "**Remedy**")^{[55][121]}
- Vodafone Cable (codenamed "**Gerontic**")^{[55][121]}
- Global Crossing (codenamed "**Pinnage**")^{[55][121]}
- Level 3 (codenamed "**Little**")^{[55][121]}
- Viatel (codenamed "**Vitreous**")^{[55][121]}
- Interoute (codenamed "**Streetcar**")^{[55][121]}

Each of them were assigned a particular area of the international fiber-optic network for which they were individually responsible. The following networks have been infiltrated by the GCHQ: TAT-14 (Europe-USA), Atlantic Crossing 1 (Europe-USA), Circe South (France-UK), Circe North (The Netherlands-UK), Flag Atlantic-1, Flag Europa-Asia, SEA-ME-WE 3 (Southeast Asia-Middle East-Western Europe), SEA-ME-WE 4 (Southeast Asia-Middle East-Western Europe), Solas (Ireland-UK), UK-France 3, UK-Netherlands 14, ULYSSES (Europe-UK), Yellow (UK-USA) and Pan European Crossing.^[122]

Telecommunication companies who participated were "forced" to do so and had "no choice in the matter".^[122] Some of the companies were subsequently paid by GCHQ for their participation in the infiltration of the cables.^[122] According to the SZ the GCHQ has access to the majority of internet and telephone communications flowing throughout Europe, can listen to phone calls, read emails and text messages, see which websites internet users from all around the world are visiting. It can also retain and analyse nearly the entire European internet traffic.^[122]

The GCHQ is collecting all data transmitted to and from the United Kingdom and Northern Europe via the undersea fibre optic telecommunications cable SEA-ME-WE 3. The Security and Intelligence Division (**SID**) of Singapore co-operates with Australia in accessing and sharing communications carried by the SEA-ME-WE-3 cable. The Australian Signals Directorate (**ASD**) is also in a partnership with British, American and Singaporean intelligence agencies to tap undersea fibre optic telecommunications cables that link Asia, the Middle East and Europe and carry much of Australia's international phone and internet traffic.^[123]

The U.S. runs a top-secret surveillance program known as the **Special Collection Service (SCS)**, which is based in over 80 U.S. consulates and embassies worldwide.^{[124][125]} The NSA hacked the United Nations' video conferencing system in Summer 2012 in violation of a UN agreement.^{[124][125]}

The NSA is not just intercepting the communications of Americans who are in direct contact with foreigners targeted overseas, but also searching the contents of vast amounts of e-mail and text communications into and out of the country by Americans who mention information about foreigners under surveillance.^[126] It also spied on the Al Jazeera and gained access to its internal communications systems.^[127]

The NSA has built a surveillance network that has the capacity to reach roughly 75% of all U.S. Internet traffic.^{[128][129][130]} U.S. Law-enforcement agencies use tools used by computer hackers to gather information on suspects.^{[131][132]} An internal NSA audit from May 2012 identified 2776 incidents i.e. violations of the rules or court orders for surveillance of Americans and foreign targets in the U.S. in the period from April 2011 through March 2012, while U.S. officials stressed that any mistakes are not intentional.^{[133][134][135][136][137][138][139]}

The FISA Court that is supposed to provide critical oversight of the U.S. government's vast spying programs has limited ability to do and it must trust the government to report when it improperly spies on Americans.^[140] A legal opinion declassified on August 21, 2013 revealed that the NSA intercepted for three years as many as 56,000 electronic communications a year of Americans who weren't suspected of having links to terrorism, before FISC court that oversees surveillance found the operation unconstitutional in 2011.^{[141][142][143]}^{[144][145]} Under the **Corporate Partner Access** project, major U.S. telecommunications providers receive hundreds of millions of dollars each year from the NSA.^[146] Voluntary cooperation between the NSA and the providers of global communications took off during the 1970s under the cover name **BLARNEY**.^[146]

A letter drafted by the Obama administration specifically to inform Congress of the government's mass collection of Americans' telephone communications data was withheld from lawmakers by leaders of the House Intelligence Committee in the months before a key vote affecting the future of the program.^{[147][148]}

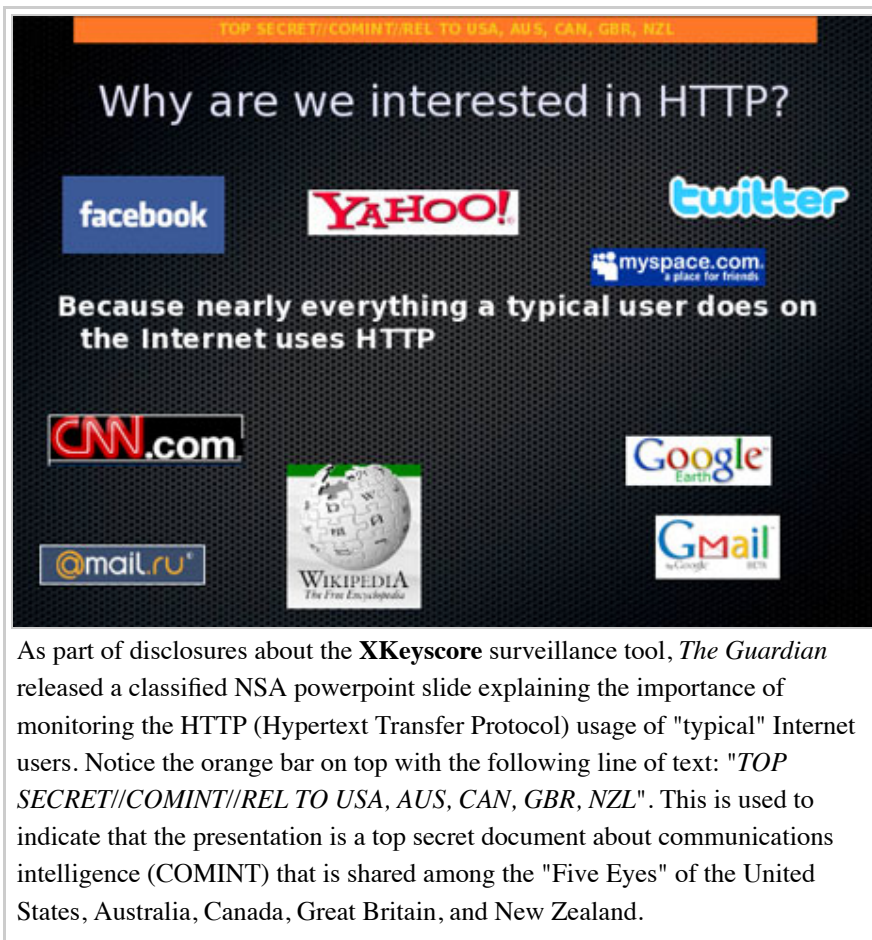
The NSA paid GCHQ over £100 Million between 2009 and 2012, in exchange for these funds GCHQ "must pull its weight and be seen to pull its weight." Documents referenced in the article explain that the weaker British laws regarding spying are "a selling point" for the NSA. GCHQ is also developing the technology to "exploit any mobile phone at any time."^[149] The NSA has under a legal authority a secret backdoor into its databases gathered from large Internet companies enabling it to search for U.S. citizens' email and phone calls without a warrant.^{[150][151]}

The Privacy and Civil Liberties Oversight Board urged the U.S. intelligence chiefs to draft stronger US surveillance guidelines on domestic spying after finding that several of those guidelines have not been updated up to 30 years.^{[152][153]} U.S. intelligence analysts have deliberately broken rules designed to prevent them from spying on Americans by choosing to ignore so-called "minimisation procedures" aimed at protecting privacy.^{[154][155][156]}

After the U.S. Foreign Secret Intelligence Court ruled in October 2011 that some of the NSA's activities were unconstitutional, the agency paid millions of dollars to major internet companies to cover extra costs incurred in their involvement with the **PRISM** surveillance program.^[157]

"Mastering the Internet" (MTI) is part of the Interception Modernisation Programme (IMP) of the British government that involves the insertion of thousands of DPI (deep packet inspection) "black boxes" at various internet service providers, as revealed by the British media in 2009.^[158]

In 2013, it was further revealed that the NSA had made a £17.2 million financial contribution to the project, which is capable of vacuuming signals from up to 200 fibre-optic cables at all physical points of entry into Great Britain.^[159]



September

The *Guardian* and the *New York Times* reported on secret documents leaked by Snowden showing that the NSA has been in "collaboration with technology companies" as part of "an aggressive, multipronged effort" to weaken the encryption used in commercial software, and the GCHQ has a team dedicated to cracking "Hotmail, Google, Yahoo and Facebook" traffic.^{[160][161][162][163][164][165]} Israel, Sweden and Italy are also cooperating with American and British intelligence agencies. Under a secret treaty codenamed "**Lustre**", French intelligence agencies transferred millions of metadata records to the NSA.^{[63][64][166][167]}

A special branch of the NSA called "**Follow the Money**" (FTM) monitors international payments, banking and credit card transactions and later stores the collected data in the NSA's own financial databank "**Tracfin**".^[168] The NSA monitored the communications of Brazil's president Dilma Rousseff and her top aides.^[169] The agency also spied on Brazil's oil firm Petrobras as well as French diplomats, and gained access to the private network of the Ministry of Foreign Affairs of France and the SWIFT network.^[170]

In the United States, the NSA uses the analysis of phone call and e-mail logs of American citizens to create sophisticated graphs of their social connections that can identify their associates, their locations at certain times, their traveling companions and other personal information.^[171] The NSA routinely shares raw intelligence data with Israel without first sifting it to remove information about U.S. citizens.^{[7][172]}

In an effort codenamed **GENIE**, computer specialists can control foreign computer networks using "covert implants," a form of remotely transmitted malware on tens of thousands of devices annually.^{[173][174][175][176]}

As worldwide sales of smartphones began exceeding those of feature phones, the NSA decided to take advantage of the smartphone boom. This is particularly advantageous because the smartphone combines a myriad of data that would interest an intelligence agency, such as social contacts, user behavior, interests, location, photos and credit card numbers and passwords.^[177]

An internal NSA report from 2010 stated that the spread of the smartphone has been occurring "extremely rapidly" —developments that "certainly complicate traditional target analysis."^[177] According to the document, 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.^[177] Similarly, Britain's GCHQ assigned a team to study and crack the BlackBerry.^[177]

Under the heading "iPhone capability", the document notes that 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.^[177]

On September 9, 2013, an internal NSA presentation on iPhone Location Services was leaked by Der Spiegel^[178]



Who knew in 1984...



...that this would be big brother...



...and the zombies would be paying customers?^[178]

October

On October 4, 2013, *The Washington Post* and *The Guardian* jointly reported that the NSA and the GCHQ have made repeated attempts to spy on anonymous Internet users who have been communicating in secret via the anonymity network Tor. Several of these surveillance operations involve the implantation of malicious code into the computers of Tor users who visit particular websites. The NSA and GCHQ have partly succeeded in blocking access to the anonymous network, diverting Tor users to insecure channels. The government agencies were also able to uncover the identity of some anonymous Internet users.^{[179][180][181][182][183][184][185][186][187]}

The Communications Security Establishment Canada (**CSEC**) has been using a program called **Olympia** to map the communications of Brazil's Mines and Energy Ministry by targeting the metadata of phone calls and emails to and from the ministry.^{[188][189]}

The Australian Federal Government knew about the PRISM surveillance program months before Edward Snowden made details public.^{[190][191]}

The NSA monitored the public email account of former Mexican president Felipe Calderón (thus gaining access to the communications of high ranking cabinet members), the E-Mails of several high-ranking members of Mexico's security forces and text and the mobile phone communication of current Mexican president Enrique Peña Nieto.^{[192][193]} The NSA tries to gather cellular and landline phone numbers—often obtained from American diplomats—for as many foreign officials as possible. The contents of the phone calls are stored in computer databases that can regularly be searched using keywords.^{[194][195]}

The NSA has been monitoring telephone conversations of 35 world leaders.^[196] The U.S. government's first public acknowledgment that it tapped the phones of world leaders was reported on October 28, 2013 by the Wall Street Journal after an internal U.S. government review turned up NSA monitoring of some 35 world leaders.^[197] The GCHQ has tried to keep its mass surveillance program a secret because it feared a "damaging public debate" on the scale of its activities which could lead to legal challenges against them.^[198]

The Guardian revealed that the NSA had been monitoring telephone conversations of 35 world leaders after being given the numbers by an official in another U.S. government department. A confidential memo revealed that the NSA encouraged senior officials in such Departments as the White House, State and The Pentagon, to share their "Rolodexes" so the agency could add the telephone numbers of leading foreign politicians to their surveillance systems. Reacting to the news, German leader Angela Merkel, arriving in Brussels for an EU summit, accused the U.S. of a breach of trust, saying: "We need to have trust in our allies and partners, and this must now be established once again. I repeat that spying among friends is not at all acceptable against anyone, and that goes for every citizen in Germany."^[196] The NSA collected in 2010 data on ordinary Americans' cellphone locations, but later discontinued it because it had no "operational value."^[199]

Under Britain's **MUSCULAR** programme, the NSA and the GCHQ have secretly broken into the main communications links that connect Yahoo and Google data centers around the world and thereby gained the ability to collect metadata and content at will from hundreds of millions of user accounts.^{[200][201][202][203][204]}

The mobile phone of German Chancellor Angela Merkel might have been tapped by U.S. intelligence.^{[205][206][207][208][209][210][211]} According to the Spiegel this monitoring goes back to 2002^{[212][213][214]} and ended in the summer of 2013,^[197] while the New York Times reported that Germany has evidence that the NSA's

surveillance of Merkel began during George W. Bush's tenure.^[215] After learning from *Der Spiegel* magazine that the NSA has been listening in to her personal mobile phone, Merkel compared the snooping practices of the NSA with those of the Stasi.^[216]

On October 31, 2013, Hans-Christian Ströbele, a member of the German Bundestag, met Snowden in Moscow and revealed the former intelligence contractor's readiness to brief the German government on NSA spying.^[217]

A highly sensitive signals intelligence collection program known as **Stateroom** involves the interception of radio, telecommunications and internet traffic. It is operated out of the diplomatic missions of the Five Eyes (Australia, Britain, Canada, New Zealand, United States) in numerous locations around the world. The program conducted at U.S. diplomatic missions is run in concert by the U.S. intelligence agencies NSA and CIA in a joint venture group called "**Special Collection Service**" (SCS), whose members work undercover in shielded areas of the American Embassies and Consulates, where they are officially accredited as diplomats and as such enjoy special privileges. Under diplomatic protection, they are able to look and listen unhindered. The SCS for example used the American Embassy near the Brandenburg Gate in Berlin to monitor communications in Germany's government district with its parliament and the seat of the government.^{[211][218][219][220]}

Under the **Stateroom** surveillance programme, Australia operates clandestine surveillance facilities to intercept phone calls and data across much of Asia.^{[219][221]}

In France, the NSA targeted people belonging to the worlds of business, politics or French state administration. The NSA monitored and recorded the content of telephone communications and the history of the connections of each target i.e. the metadata.^{[222][223]} The actual surveillance operation was performed by French intelligence agencies on behalf of the NSA.^{[63][224]} The cooperation between France and the NSA was confirmed by the Director of the NSA, Keith B. Alexander, who asserted that foreign intelligence services collected phone records in "war zones" and "other areas outside their borders" and provided them to the NSA.^[225]

The French newspaper *Le Monde* also disclosed new PRISM and Upstream slides (See Page 4, 7 and 8) coming from the "PRISM/US-984XN Overview" presentation.^[226]

In Spain, the NSA intercepted the telephone conversations, text messages and emails of millions of Spaniards, and spied on members of the Spanish government.^[227] Between December 10, 2012 and January 8, 2013, the NSA collected metadata on 60 million telephone calls in Spain.^[228]

According to documents leaked by Snowden, the surveillance of Spanish citizens was jointly conducted by the NSA and the intelligence agencies of Spain.^{[229][230]}

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) What is TOR?

- (U) “The Onion Router”
- (U) Enables anonymous internet activity
 - General privacy
 - Non-attribution
 - Circumvention of nation state internet policies
- (U) Hundreds of thousands of users
 - Dissidents (Iran, China, etc)
 - (S//SI//REL) **Terrorists!**
 - (S//SI//REL) Other targets too!

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

On October 4, 2013, *The Washington Post* published a powerpoint presentation leaked by Snowden, showing how the NSA has compromised the Tor encrypted network that is being employed by hundreds of thousands of people to circumvent "nation state internet policies". By secretly exploiting a JavaScript plug-in, the NSA is able to uncover the identities of various anonymous Internet users such as dissidents, terrorists, and other targets

November

The *New York Times* reported that the NSA carries out an eavesdropping effort, dubbed Operation Dreadnought, against the Iranian leader Ayatollah Ali Khamenei. During his 2009 visit to Iranian Kurdistan, the agency collaborated with the GCHQ and the U.S.'s National Geospatial-Intelligence Agency, collecting radio transmissions between aircraft and airports, examining Khamenei's convoy with satellite imagery, and enumerating military radar stations. According to the story, an objective of the operation is "communications fingerprinting": the ability to distinguish Khamenei's communications from those of other people in Iran.^[231]

The same story revealed an operation code-named Ironavenger, in which the NSA intercepted e-mails sent between a country allied with the United States and the government of "an adversary". The ally was conducting a spear-phishing attack: its e-mails contained malware. The NSA gathered documents and login credentials belonging to the enemy country, along with knowledge of the ally's capabilities for attacking computers.^[231]

According to the British newspaper *The Independent*, the British intelligence agency GCHQ maintains a listening post on the roof of the British Embassy in Berlin that is capable of intercepting mobile phone calls, wi-fi data and long-distance communications all over the German capital, including adjacent government buildings such as the Reichstag (seat of the German parliament) and the Chancellery (seat of Germany's head of government) clustered around the Brandenburg Gate.^[232]

Operating under the code-name "Quantum Insert", the GCHQ set up a fake website masquerading as LinkedIn, a social website used for professional networking, as part of its efforts to install surveillance software on the computers of the telecommunications operator Belgacom.^[233] In addition, the headquarters of the oil cartel OPEC were infiltrated by the GCHQ as well as the NSA, which bugged the computers of nine OPEC employees and monitored the General Secretary of OPEC.^[233]

For more than three years the GCHQ has been using an automated monitoring system code-named "Royal Concierge" to infiltrate the reservation systems of at least 350 upscale hotels in many different parts of the world in order to target, search and analyze reservations to detect diplomats and government officials.^[234] First tested in 2010, the aim of the "Royal Concierge" is to track down the travel plans of diplomats, and it is often supplemented with surveillance methods related to human intelligence (HUMINT). Other covert operations include 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.^[234]

In November 2013, the Australian Broadcasting Corporation and *The Guardian* revealed that the Australian Signals Directorate (**DSD**) had attempted to listen to the private phone calls of the president of Indonesia and his wife. The Indonesian foreign minister, Marty Natalegawa, confirmed that he and the president had contacted the ambassador in Canberra. Natalegawa said any tapping of Indonesian politicians' personal phones "violates every single decent and legal instrument I can think of—national in Indonesia, national in Australia, international as well".^[235]

Other high ranking Indonesian politicians targeted by the DSD include:

- Boediono^[236] (Vice President)
- Jusuf Kalla^[236] (Former Vice President)
- Dino Patti Djalal^[236] (Ambassador to the United States)
- Andi Mallarangeng^[236] (Government spokesperson)
- Hatta Rajasa^[236] (State Secretary)
- Sri Mulyani Indrawati^[236] (Former Finance Minister and current managing director of the World Bank)
- Widodo Adi Sutjipto^[236] (Former Commander-in-Chief of the military)
- Sofyan Djalil^[236] (Senior government advisor)

Carrying the title "3G impact and update", a classified presentation leaked by Snowden revealed the attempts of the ASD/DSD to keep up to pace with the rollout of 3G technology in Indonesia and across Southeast Asia. The ASD/DSD motto placed at the bottom of each page reads: "Reveal their secrets—protect our own."^[236]

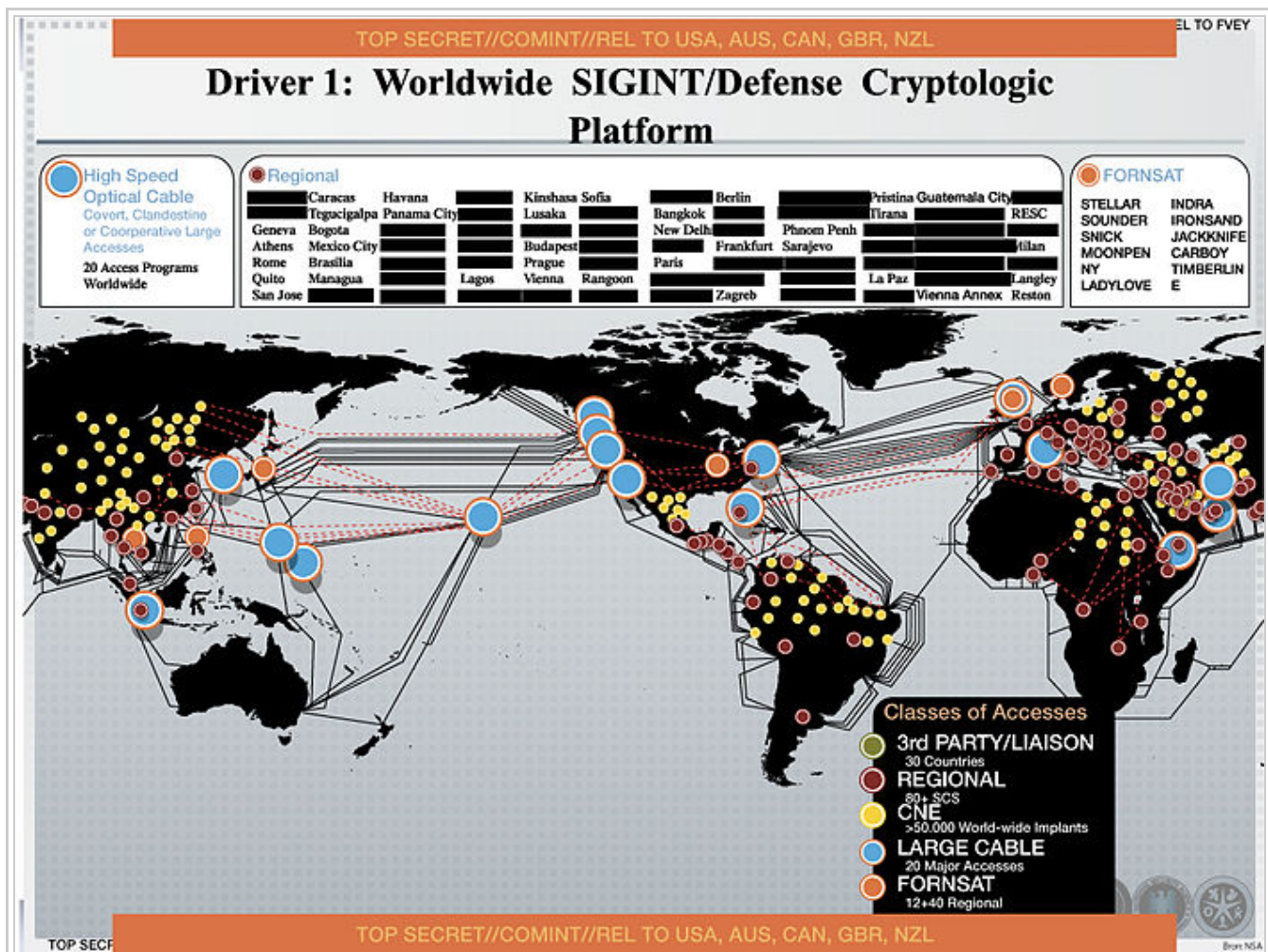
Under a secret deal approved by British intelligence officials, the NSA has been storing and analyzing the internet and email records of UK citizens since 2007. The NSA also proposed in 2005 a procedure for spying on the citizens of the UK and other Five-Eyes nations alliance, even where the partner government has explicitly denied the U.S. permission to do so. Under the proposal, partner countries must neither be informed about this particular type of surveillance, nor the procedure of doing so.^[41]

Towards the end of November, *The New York Times* released an internal NSA report outlining the agency's efforts to expand its surveillance abilities.^[237] The five-page document asserts that the law of the United States has not kept up with the needs of the NSA to conduct mass surveillance in the "golden age" of signals intelligence, but there are grounds for optimism because, in the NSA's own words:

"The culture of compliance, which has allowed the American people to entrust NSA with extraordinary authorities, will not be compromised in the face of so many demands, even as we aggressively pursue legal authorities..."^[238]

The report, titled "SIGINT Strategy 2012–2016", also said that the U.S. will try to influence the "global commercial encryption market" through "commercial relationships", and emphasized the need to "revolutionize" the analysis of its vast data collection to "radically increase operational impact".^[237]

On November 23, 2013, the Dutch newspaper *NRC Handelsblad* reported that the Netherlands was targeted by U.S. intelligence agencies in the immediate aftermath of World War II. This period of surveillance lasted from 1946 to 1968, and also included the interception of the communications of other European countries including Belgium, France, West Germany and Norway.^[239] The Dutch Newspaper also reported that NSA infected more than 50,000 computer networks worldwide, often covertly, with malicious spy software, sometimes in cooperation with local authorities, designed to steal sensitive information .^{[44][240]}



On November 23, 2013, the Dutch newspaper *NRC Handelsblad* released a top secret NSA presentation leaked by Snowden, showing five "Classes of Accesses" that the NSA uses in its worldwide signals intelligence operations.^{[44][240]} These five "Classes of Accesses" are:

☐ **3rd PARTY/LIAISON**—refers to data provided by the international partners of the NSA. Within the framework of the UKUSA Agreement, these international partners are known as "third parties".

☐ **REGIONAL**—refers to over 80 regional Special Collection Services (SCS). The SCS is a black budget program operated by the NSA and the CIA, with operations based in many cities such as Athens, Bangkok, Berlin, Brasília, Budapest, Frankfurt, Geneva, Lagos, Milan, New Delhi, Paris, Prague, Vienna, and Zagreb, and others, targeting Central America, the Arabian Peninsula, East Asia, and Continental Europe.

☐ **CNE**—an abbreviation for "Computer Network Exploitation". It is performed by a special cyber-warfare unit of the NSA known as Tailored Access Operations (TAO), which infected over 50,000 computer networks worldwide with malicious software designed to steal sensitive information, and is mostly aimed at Brazil, China, Egypt, India, Mexico, Saudi Arabia, and parts of Eastern Europe

☐ **LARGE CABLE**—20 major points of accesses, many of them located within the United States

☐ **FORNSAT**—an abbreviation for "Foreign Satellite Collection". It refers to intercepts from satellites that process data used by other countries such as Britain, Norway, Japan, and the Philippines

December

According to the classified documents leaked by Snowden, the Australian Signals Directorate, formerly known as the Defence Signals Directorate, had offered to share information on Australian citizens with the other intelligence agencies of the UKUSA Agreement. Data shared with foreign countries include "bulk, unselected, unminimised metadata" such as "medical, legal or religious information".^[241]

The Washington Post revealed that the NSA has been tracking the locations of mobile phones from all over the world by tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones. In the process of doing so, the NSA collects more than five billion records of phone locations on a daily basis. This enables NSA analysts to map cellphone owners' relationships by correlating their patterns of movement over time with thousands or millions of other phone users who cross their paths.^{[242][243][244][245][246][247][248][249]}

The Washington Post also reported that the NSA makes use of location data and advertising tracking files generated through normal internet browsing i.e. tools that enable Internet advertisers to track consumers from Google and others to get information on potential targets, to pinpoint targets for government hacking and to bolster surveillance.^{[250][251][252]}

The Norwegian Intelligence Service (NIS), which cooperates with the NSA, 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".^[253] A top secret memo of the NSA lists the following years as milestones of the **Norway-United States of America SIGINT agreement**, or NORUS Agreement:

- **1952** - Informal starting year of cooperation between the NIS and the NSA^[254]
- **1954** - Formalization of the agreement^[254]
- **1963** - Extension of the agreement for coverage of foreign instrumentation signals intelligence (FISINT)^[254]
- **1970** - Extension of the agreement for coverage of electronic intelligence (ELINT)^[254]
- **1994** - Extension of the agreement for coverage of communications intelligence (COMINT)^[254]

The NSA considers the NIS to be 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 from the NIS.^[254]

On 5 December, Sveriges Television (*Swedish Television*) reported that the National Defence Radio Establishment of Sweden (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.^{[255][256]} The Swedish-American surveillance operation also targeted Russian energy interests as well as the Baltic states.^[257] As part of the UKUSA Agreement, a secret treaty was signed in 1954 by Sweden with the United States, the United Kingdom, Canada, Australia and New Zealand, regarding collaboration and intelligence sharing.^[258]

As a result of Snowden's disclosures, the notion of Swedish neutrality in international politics has been called into question. In an internal document dating from the year 2006, the NSA acknowledged that its "relationship" with Sweden is "protected at the TOP SECRET level because of that nation's political neutrality."^[259] Specific details of Sweden's cooperation with members of the UKUSA Agreement include:

- The FRA has been granted access to XKeyscore, an analytical database of the NSA.^[260]

- Sweden updated the NSA on changes in Swedish legislation that provided the legal framework for information sharing between the FRA and the Swedish Security Service.^[52]
- Since January 2013, a counterterrorism analyst of the NSA has been stationed in the Swedish capital of Stockholm^[52]
- Several years before the Riksdag of Sweden passed the controversial FRA law, which allows the FRA to warrantlessly wiretap all telephone and Internet traffic that crosses Sweden's borders, the NSA, the GCHQ and the FRA signed an agreement in 2004 that allows the FRA to directly collaborate with the NSA without having to consult the GCHQ.^[52]

In order to identify targets for government hacking and surveillance, both the GCHQ and the NSA have used advertising cookies operated by Google, known as Pref, to "pinpoint" targets. According to documents leaked by Snowden, the Special Source Operations of the NSA has been sharing information containing "logins, cookies, and GooglePREFID" with the Tailored Access Operations division of the NSA, as well as Britain's GCHQ agency.^[261]

During the 2010 G-20 Toronto summit, the U.S. embassy in Ottawa was transformed into a security command post during a six-day spying operation that was conducted by the NSA and closely co-ordinated with the Communications Security Establishment Canada (CSEC). The goal of the spying operation was, among others, to obtain information on international development, banking reform, and to counter trade protectionism to support "U.S. policy goals."^[262] On behalf of the NSA, the CSEC has set up covert spying posts in 20 countries around the world.^[10]

In Italy the Special Collection Service of the NSA maintains two separate surveillance posts in Rome and Milan.^[263] According to a secret NSA memo dated September 2010, the Italian embassy in Washington, D.C. has been targeted by two spy operations of the NSA:

- Under the codename "Bruneau", which refers to mission "Lifesaver", the NSA sucks out all the information stored in the embassy's computers and creates electronic images of hard disk drives.^[263]
- Under the codename "Hemlock", which refers to mission "Highlands", the NSA gains access to the embassy's communications through physical "implants".^[263]

Due to concerns that terrorist or criminal networks may be secretly communicating via computer games, the NSA, the GCHQ, the CIA, and the FBI have been conducting surveillance and scooping up data from 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.^{[264][265][266][267]}

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.^[268] 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.^[269]

US district court judge for the District of Columbia, Richard Leon, declared^{[270][271][272][273][274][275]} on December 16, 2013, that the mass collection of metadata of Americans' telephone records by the National Security Agency probably violates the fourth amendment prohibition of unreasonable searches and seizures.^[276] Leon granted the request for a preliminary injunction that blocks the collection of phone data for

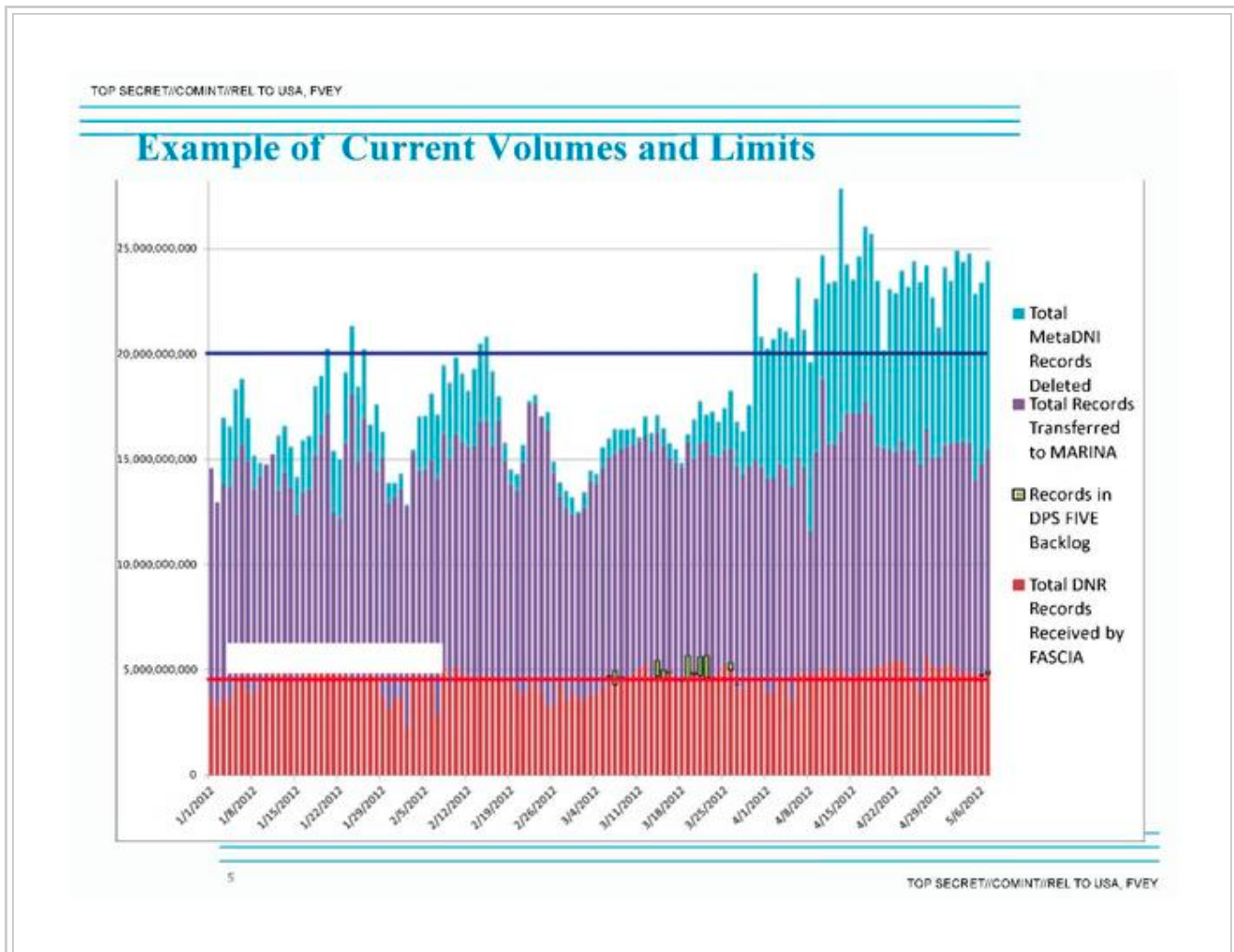
two private plaintiffs (Larry Klayman, a conservative lawyer, and Charles Strange, father of a cryptologist killed in Afghanistan when his helicopter was shot down in 2011)^[277] and ordered the government to destroy any of their records that have been gathered. But the judge stayed action on his ruling pending a government appeal, recognizing in his 68-page opinion the “significant national security interests at stake in this case and the novelty of the constitutional issues.”^[276]

However federal judge William H. Pauley III in New York City ruled^[278] the U.S. government’s global telephone data-gathering system is needed to thwart potential terrorist attacks, and that it can only work if everyone’s calls are swept in. U.S. District Judge Pauley also ruled that Congress legally set up the program and that it does not violate anyone’s constitutional rights. The judge also concluded that the telephone data being swept up by NSA did not belong to telephone users, but to the telephone companies. He further ruled that when NSA obtains such data from the telephone companies, and then probes into it to find links between callers and potential terrorists, this further use of the data was not even a search under the Fourth Amendment. He also concluded that the controlling precedent is *Smith v. Maryland*: “Smith’s bedrock holding is that an individual has no legitimate expectation of privacy in information provided to third parties,” Judge Pauley wrote.^{[279][280][281][282]} The American Civil Liberties Union declared on January 2, 2012 that it will appeal Judge Pauley's ruling that NSA bulk the phone record collection is legal. "The government has a legitimate interest in tracking the associations of suspected terrorists, but tracking those associations does not require the government to subject every citizen to permanent surveillance," deputy ACLU legal director Jameel Jaffer said in a statement.^[283]

In recent years, American and British intelligence agencies conducted surveillance on more than 1,100 targets, including the office of an Israeli prime minister, heads of international aid organizations, foreign energy companies and a European Union official involved in antitrust battles with American technology businesses.^[284]

A catalog of high-tech gadgets and software developed by the NSA's Tailored Access Operations (TAO) was leaked by the German news magazine *Der Spiegel*.^[285] Dating from 2008, the catalog revealed the existence of special gadgets modified to capture computer screenshots and USB flash drives secretly fitted with radio transmitters to broadcast stolen data over the airwaves, and fake base stations intended to intercept mobile phone signals, as well as many other secret devices and software implants listed here:

The Tailored Access Operations (TAO) division of the NSA intercepted the shipping deliveries of computers and laptops in order to install spyware and physical implants on electronic gadgets. This was done in close cooperation with the FBI and the CIA.^{[285][286][287][288][289][290][291]} NSA officials responded to the *Spiegel* reports with a statement, which said: "Tailored Access Operations is a unique national asset that is on the front lines of enabling NSA to defend the nation and its allies. [TAO's] work is centred on computer network exploitation in support of foreign intelligence collection."^[292]



On 4 December 2013, *The Washington Post* released an internal NSA chart illustrating the extent of the agency's mass collection of mobile phone location records, which amounts to about five billion on a daily basis.^[242] The records are stored in a huge database known as **FASCIA**, which received over 27 terabytes of location data within seven months.^[293]

Also in December the French Trésor public, which also runs a certificate authority, was found to have issued fake certificates impersonating Google in order to facilitate spying on French government employees via man-in-the-middle attacks.^[294]

2014

January

The NSA is working to build a powerful quantum computer capable of breaking all types of encryption.

^{[295][296][297][298][299]} The effort is part of a US\$79.7 million research program known as "**Penetrating Hard Targets**". It involves extensive research carried out in large, shielded rooms known as Faraday cages, which are designed to prevent electromagnetic radiation from entering or leaving.^[296] Currently, the NSA is close to producing basic building blocks that will allow the agency to gain "complete quantum control on two semiconductor qubits".^[296] Once a quantum computer is successfully built, it would enable the NSA to unlock

the encryption that protects data held by banks, credit card companies, retailers, brokerages, governments and health care providers.^[295]

According to the New York Times the NSA is monitoring approximately 100.000 computers worldwide with spy software named Quantum. Quantum enables the NSA to conduct surveillance on those computers on the one hand and can also create a digital highway for launching cyberattacks on the other hand. Among the targets are the Chinese and Russian military, but also trade institutions within the European Union. The NYT also reported that the NSA can access and alter computers which are not connected with the internet by a secret technology in use by the NSA since 2008. The prerequisite is the physically insertion of the radio frequency hardware by a spy, a manufacturer or an unwitting user. The technology relies on a covert channel of radio waves that can be transmitted from tiny circuit boards and USB cards inserted surreptitiously into the computers. In some cases, they are sent to a briefcase-size relay station that intelligence agencies can set up miles away from the target. The technology can also transmit malware back to the infected computer.^[44]

Channel 4 and *The Guardian* revealed the existence of **Dishfire**, a massive database of the NSA that collects hundreds of millions of text messages on a daily basis.^[300] The GCHQ has been given full access to the database, which it uses to obtain personal information of Britons by exploiting a legal loophole.^[301]

Each day, the database receives and stores the following amounts of data:

- Geolocation data of more than 76,000 text messages and other travel information^[302]
- Over 110,000 names, gathered from electronic business cards^[302]
- Over 800,000 financial transactions that are either gathered from text-to-text payments or by linking credit cards to phone users^[302]
- Details of 1.6 million border crossings based on the interception of network roaming alerts^[302]
- Over 5 million missed call alerts^[302]
- About 200 million text messages from around the world^[303]

The database is supplemented with an analytical tool known as the **Prefer** program, which processes SMS messages to extract other types of information including contacts from missed call alerts.^[302]

According to the New York Times,^{[304][305][306]} *The Guardian*^[307] and ProPublica^[308] by 2007, the NSA and the GCHQ began working together to collect and store data from dozens of smartphone application software. According to a 2008 GCHQ report leaked by Snowden, "anyone using Google Maps on a smartphone is working in support of a GCHQ system". The NSA and the GCHQ have traded recipes for various purposes such as grabbing location data and journey plans that are made when a target uses Google Maps, and vacuuming up address books, buddy lists, phone logs and geographic data embedded in photos posted on the mobile versions of numerous social networks such as Facebook, Flickr, LinkedIn, Twitter and other services. In a separate 20-page report dated 2012, the GCHQ cited the popular smartphone game "Angry Birds" as an example of how an application could be used to extract user data. Taken together, such forms of data collection would allow the agencies to collect vital information about a user's life, including his or her home country, current location (through geolocation), age, gender, ZIP code, marital status, income, ethnicity, sexual orientation, education level, number of children, etc.^{[309][310]}

A GCHQ document dated August 2012 provided details of the **Squeaky Dolphin** surveillance program, which enables the GCHQ based on its cable-tapping capabilities broad, real-time monitoring of various social media features and social media traffic such as YouTube video views, the Like button on Facebook, and Blogspot/Blogger visits without the knowledge or consent of the companies providing those social media features. The agency's "Squeaky Dolphin" program can collect, analyze and utilize YouTube, Facebook and Blogger data in specific situations in real time for analysis purposes. The program also collects the addresses from the billion of vidoes watched daily as well as some user information for analysis purposes.^{[167][311][312]}








On 27 January 2014, *The New York Times* released^[306] an internal NSA document from a 2010 meeting that details the extent of the agency's surveillance on smartphones. Data collected include phone settings, network connections, Web browsing history, buddy lists, downloaded documents, encryption usage, and user agents. Notice the following line of text at the bottom - "*TOP SECRET//COMINT//REL TO USA, FVEY*" - which is used to indicated that this top secret document is related to communications intelligence (COMINT), and can be accessed by the USA and its Five Eyes (FVEY) partners in Australia, Britain, Canada, and New Zealand

According to information of Edward Snowden to the Guardian and the New York Times, Angry Birds and other smartphone apps may have been targeted by the National Security Agency and its UK counterpart for user data.^{[313][314]}

Aftermath

Main article: Aftermath of the global surveillance disclosure

Reactions of political leaders

Country	Government official	Quote
 United States	President Barack Obama	" <i>There is no spying on Americans</i> " (August 7) ^{[315][316]}
	White House Press Secretary Jay Carney	" <i>They are programs that were authorized by Congress</i> " (June 13) ^[317]
	Attorney General Eric Holder	" <i>We cannot target even foreign persons overseas without a valid foreign intelligence purpose.</i> " (June 14) ^[318]
 United Kingdom	Prime Minister David Cameron	" <i>If they (the media) don't demonstrate some social responsibility it will be very difficult for government to stand back and not to act</i> " (October 28) ^[319]
	Foreign Secretary William Hague	" <i>We take great care to balance individual privacy with our duty to safeguard the public and UK national security</i> " (June 10) ^[320]
	Deputy Prime Minister Nick Clegg	" <i>You must absolutely defend the principle of secrecy for the intelligence agencies</i> " (October 10) ^[321]
 Australia	Prime Minister Tony Abbott	" <i>Every Australian governmental agency, every Australian official at home and abroad, operates in accordance with the law</i> " (October 31) ^[322]
 Germany	Chancellor Angela Merkel	" <i>A country without intelligence work would be too vulnerable.</i> " (July 10) ^[323]
	Interior Minister Hans-Peter Friedrich	" <i>The Americans take our data privacy concerns seriously.</i> " (August) ^[324]
 Sweden	Foreign Minister Carl Bildt	" <i>I am convinced that it is a national necessity for Sweden to have a well-functioning intelligence service</i> " (December 13) ^[325]

Review of intelligence agencies

Germany

In July 2013, the German government announced an extensive review of Germany's intelligence services.^{[326][327]}

United States

In August 2013, the U.S. government announced an extensive review of U.S. intelligence services.^{[328][329]}

United Kingdom

In October 2013, the British government announced an extensive review of British intelligence services.^[330]

Canada

In December 2013, the Canadian government announced an extensive review of Canada's intelligence services.^[331]

Criticism

In January 2014 U.S. President Barack Obama said that "the sensational way in which these disclosures have come out has often shed more heat than light"^[27] and critics such as Sean Wilentz claimed that "the NSA has acted far more responsibly than the claims made by the leakers and publicized by the press." In Wilentz' view "The leakers have gone far beyond justifiably blowing the whistle on abusive programs. In addition to their alarmism about [U.S.] domestic surveillance, many of the Snowden documents released thus far have had nothing whatsoever to do with domestic surveillance."^[28] Edward Lucas, former Moscow bureau chief for *The Economist*, agreed, asserting that "Snowden's revelations neatly and suspiciously fits the interests of one country: Russia" and citing Masha Gessen's statement that "The Russian propaganda machine has not gotten this much mileage out of a US citizen since Angela Davis's murder trial in 1971."^[332]

Bob Cesca objected to the *New York Times* failing to redact the name of a NSA employee and the specific location where an al Qaeda group was being targeted in a series of slides the paper made publicly available.^[333]

Russian journalist Andrei Soldatov argued that Snowden's revelations had had negative consequences for internet freedom in Russia, as Russian authorities increased their own surveillance on and regulation of the use of U.S. based services such as Google and Facebook on the pretext of protecting the privacy of Russian users. Soldatov said that as a result of the disclosures, international support for having national governments take over the powers of the organizations involved in coordinating the Internet's global architectures had grown, which could lead to a Balkanization of the Internet that restricted free access to information.^[334] The Montevideo Statement on the Future of Internet Cooperation issued in October 2013 by ICANN and other organizations warned against "Internet fragmentation at a national level" and expressed "strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations".^[335]

Gallery

International relations



NSA's relationship with Norway's NIS



NSA's relationship with Sweden's FRA



NSA's agreement to share data with Israel's ISNU



German BND's usage of the NSA's XKEYSCORE



NSA's relationship with Canada's CSEC

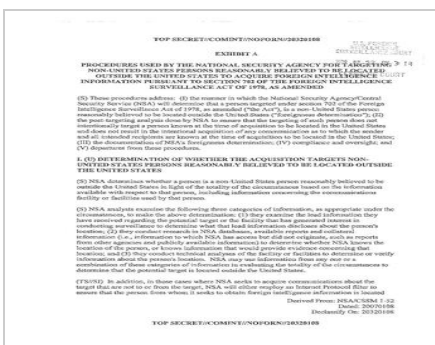


Summary of a secret meeting between the NSA and the Dutch intelligence services AIVD and MIVD

U.S. domestic federal documents



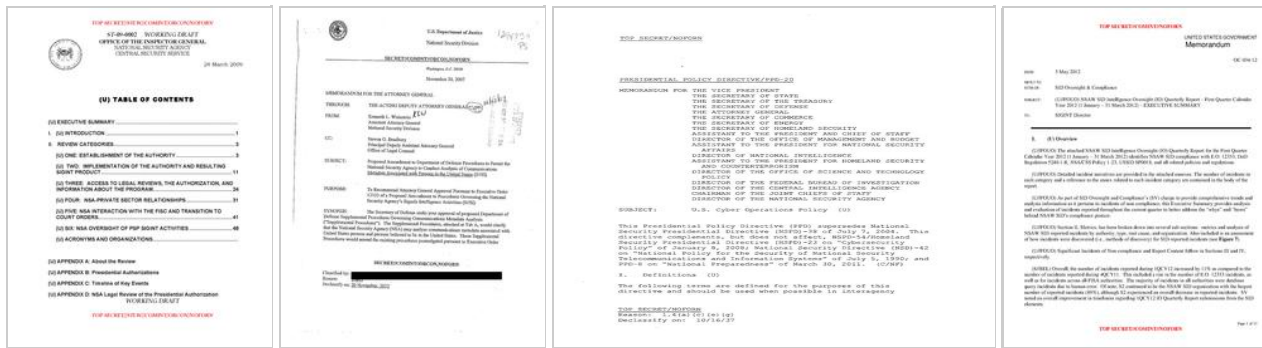
Court order demanding that Verizon hand over all metadata to NSA.



Procedures used to target Foreigners.



Procedures used to Minimize collection on US persons.

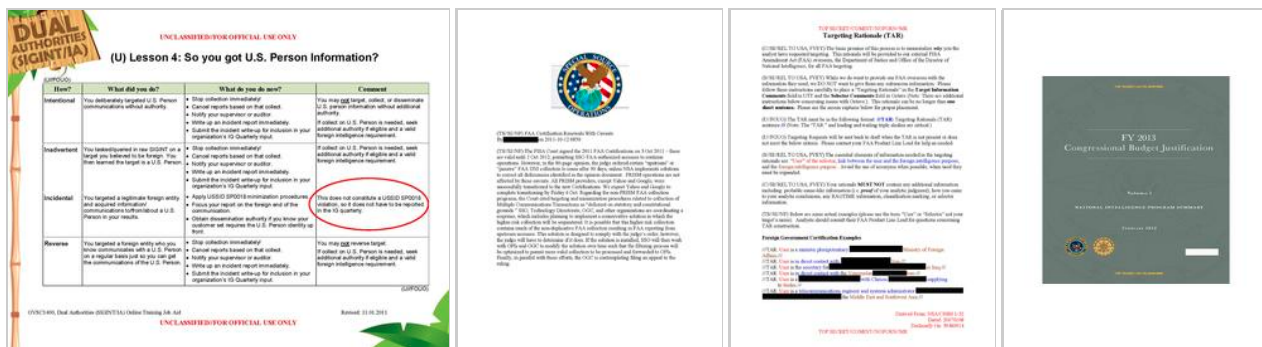


2009 OIG Draft Report on Stellar Wind.

2007 Memos by Michael Mukasey requesting Broader powers.

Presidential Policy Directive – PPD 20 Signed By Barack Obama Relating to Cyberwarfare

NSA report on privacy violations.



What's a 'privacy violation'

FISA Court finds NSA surveillance "deficient on statutory and constitutional grounds" but nonetheless recertifies it.

Targeting Rationale Guidelines

Extracts of FY 2013 Intelligence Budget, volume 1

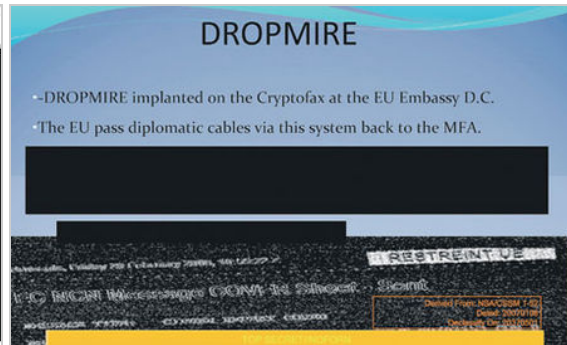
The image shows a table from the FY 2013 Intelligence Budget, titled 'FY 2013 Intelligence Budget, additional tables'. The table lists various budget items and their corresponding amounts. The columns include 'Item', 'Amount', 'Category', and 'Subcategory'. The table is organized into several sections, including 'Intelligence Community', 'Department of Defense', and 'Department of Justice'. The table is a detailed breakdown of the budget, showing the allocation of funds across different areas of intelligence and national security.

FY 2013 Intelligence Budget, additional tables

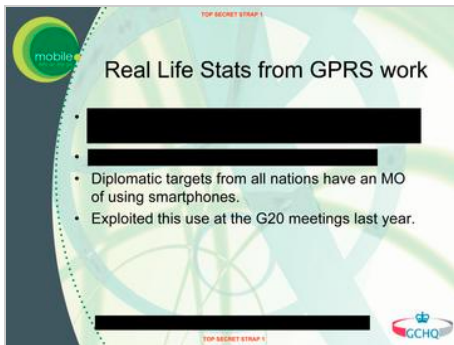
NSA presentations



SilverZephyr Slide



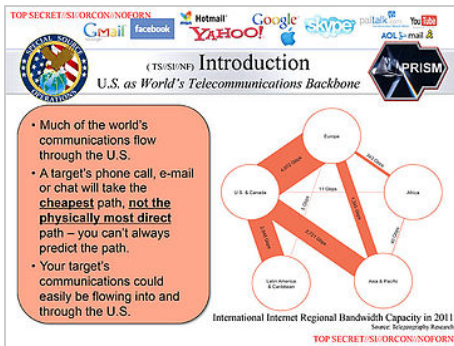
Dropmire Slide.



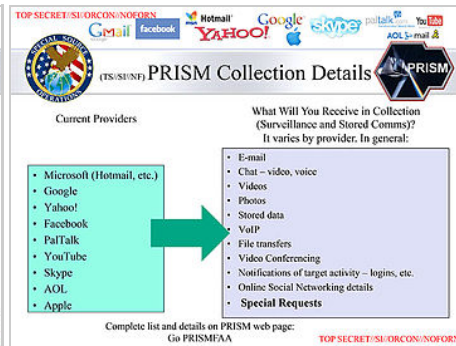
Documents relating to spying on the 2009 G20 Summit



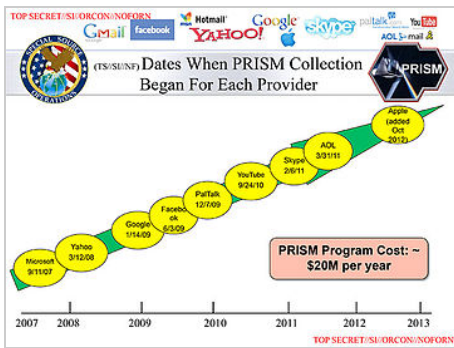
Cover page of the PRISM presentation.



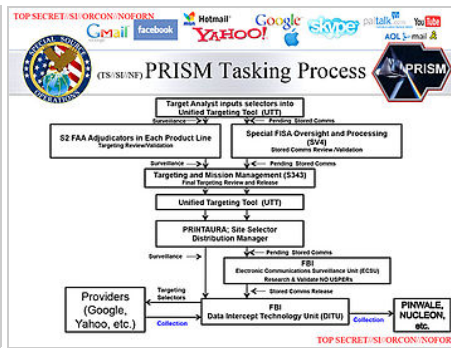
Map of global internet bandwidth.



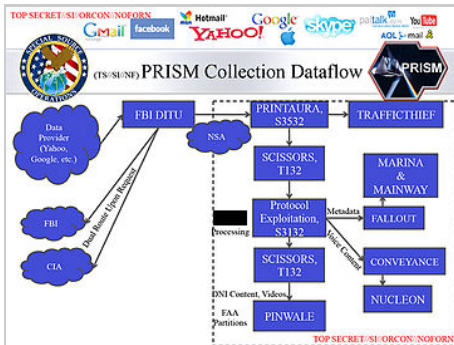
Names of the PRISM content providers and which services they typically provide.



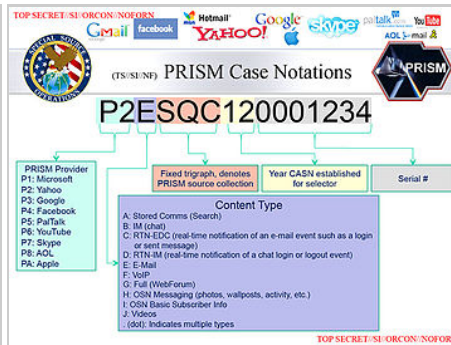
Dates each content provider was added to PRISM.



Flowchart of the PRISM tasking process.



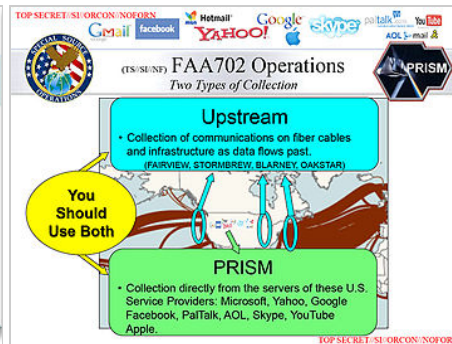
PRISM dataflow.



Explanation of PRISM case names.



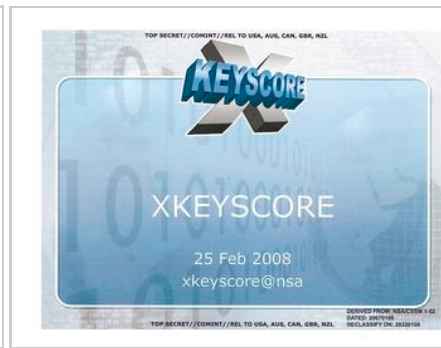
REPRISMFISA web application.



Upstream and PRISM.



A week in the life of Prism



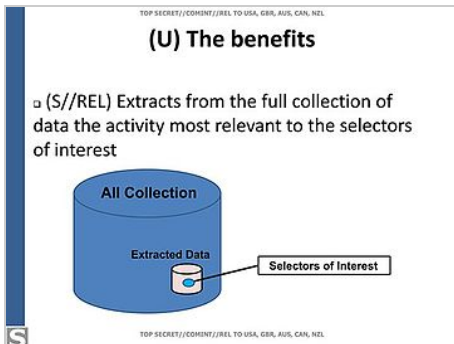
A 2008 Presentation of the XKeyscore program. (PDF, 27.26 MB)



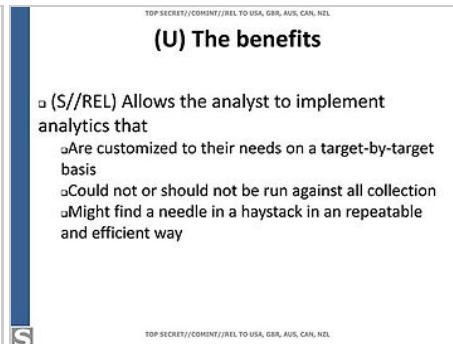
Geopolitical Trends: Key Challenges



Geopolitical trends: Global Drivers



Benefits of contact graph analysis.



Benefits of contact graph analysis.

(U) Hops

- 1-hop We may build a 1-hop graph by selecting all vertices connected to a root node
- 1.5-hop A 1.5-hop graph contains all vertices connected to a root node and all connections between those vertices

The diagram illustrates two types of graph hops. On the left, labeled '1 Hop', a central blue square node is connected to five red square nodes. On the right, labeled '1.5 Hop', the same central blue square node is connected to five red square nodes, and these red square nodes are also connected to each other, forming a more complex network.

Hops in a contact graph.

(U//FOUO) S2C41 surge effort

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Peña Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

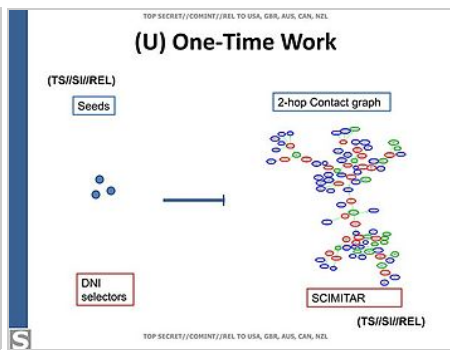
Spying against Enrique Peña Nieto and his associates.

[illegible]

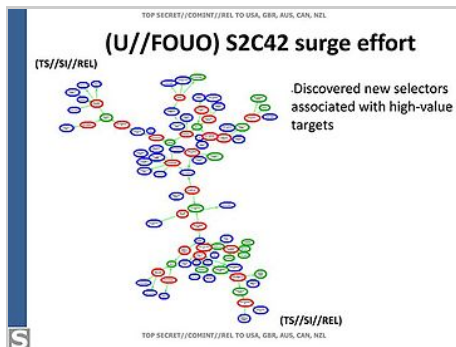
Emails from Nieto detailing potential cabinet picks.



Spying effort against Dilma Rousseff and her advisers.



Details of the process in the Rousseff operation (2 hop contact graph)



Details of the process in the Rousseff operation (2 hop contact graph)

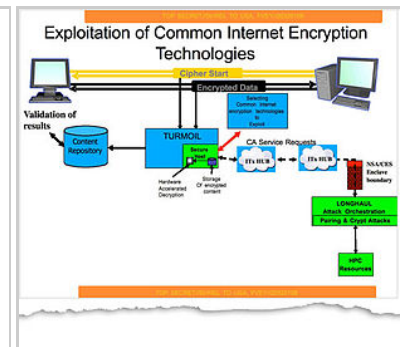
(U) Conclusion

α(S//REL) Contact graph-enhanced filtering is a simple yet effective technique, which may allow you to find previously unobtainable results and empower analytic discovery

α(TS//SI//REL) Teaming with S2C, SATC was able to successfully apply this technique against high-profile, OPSEC-savvy Brazilian and Mexican targets.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Benefits of contact graph analysis.



Exploitation of Common Internet Encryption Technologies.

Exceptionally Controlled Information

According to *The Guardian*, Exceptionally Controlled Information (ECI) refers to a classification level higher than Snowden's top secret documents.^[336] Documents classified as ECI contain the actual identities of the following NSA commercial partners operating the global surveillance network: **Artifice**, **Lithium** and **Serenade**.^[336] The name of a commercial NSA partner facility known as **Steelknight** is classified ECI and therefore not revealed in Snowden's documents.^[336]

Comparison with previous leaks

Year	Disclosure	Size	Main source(s)	Major publisher(s)
2013	Global surveillance disclosure	1.7 million documents ^[3]	Edward Snowden	<i>The Guardian</i> , <i>The New York Times</i> , <i>The Washington Post</i> , <i>Der Spiegel</i> , <i>El País</i> , <i>Le Monde</i> , <i>L'espresso</i> , <i>O Globo</i> , ProPublica, Australian Broadcasting Corporation, Canadian Broadcasting Corporation, <i>NRC Handelsblad</i> , Sveriges Television
2010	U.S. Army and U.S. State Department documents	734,885 files	Chelsea (then known as Bradley) Manning	<p><i>The Guardian</i>, <i>The New York Times</i>, <i>Der Spiegel</i>, <i>Le Monde</i>, <i>El País</i>, WikiLeaks</p> <p>The material consisted of:</p> <ul style="list-style-type: none"> ■ 1 Collateral Murder video^[337] + ■ 91,000 Afghan War diary^[338] + ■ 391,832 Iraq War logs^[339] + ■ 251,287 Secret US Embassy Cables^[340] + ■ 765 Gitmo DABs^[341] = 734,885 total.
1971	Pentagon Papers	4,100 pages	Daniel Ellsberg	<i>The New York Times</i>

See also

- Pentagon Papers
- Room 641A
- United States diplomatic cables leak

References

- ↑ Barton Gellman (24 December 2013). "Edward Snowden, after months of NSA revelations, says his mission's accomplished" (http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html). *The Washington Post*. Retrieved 25 December 2013. "Taken together, the revelations have brought to light a global surveillance system..."
- ↑ Greenwald, Glenn. "NSA collecting phone records of millions of Verizon customers daily" (<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>). *The Guardian*. Retrieved August 16, 2013. "Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama"
- ↑ ^{*a*} ^{*b*} "Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers" (<http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html>). Bloomberg. Retrieved 9 January 2014. "The Pentagon concluded that Edward Snowden committed the biggest theft of U.S. secrets in history, downloading about 1.7 million intelligence files, including information that could put personnel in jeopardy, according to lawmakers."
- ↑ "NSA Primary Sources" (<https://www EFF.org/nsa-spying/nsadocs>). Electronic Frontier Foundation. Retrieved 14 December 2013.

5. ^{*a b c d e f*} Hubert Gude, Laura Poitras and Marcel Rosenbach (August 5, 2013). "German intelligence Sends Massive Amounts of Data to the NSA" (<http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html>). *Der Spiegel*. Retrieved 14 December 2013.
6. ^{*a*} Gunnar Rensfeldt. "NSA "asking for" specific exchanges from FRA - Secret treaty since 1954" (<http://www.svt.se/ug/nsafra4>). Sveriges Television. Retrieved 14 December 2013.
7. ^{*a b c*} Glenn Greenwald, Laura Poitras and Ewen MacAskill (September 11, 2013). "NSA shares raw intelligence including Americans' data with Israel" (<http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>). *The Guardian*. Retrieved September 14, 2013.
8. ^{*a*} Tim Leslie and Mark Corcoran. "Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal" (<http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786>). Australian Broadcasting Corporation. Retrieved 18 December 2013.
9. ^{*a*} Julian Borger. "GCHQ and European spy agencies worked together on mass surveillance" (<http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden>). *The Guardian*. Retrieved 18 December 2013.
10. ^{*a b*} 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 13 December 2013.
11. ^{*a*} "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.
12. ^{*a b*} 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 18 December 2013.
13. ^{*a*} Christian Fuchs, John Goetz und Frederik Obermaier. "Verfassungsschutz beliefert NSA" (<http://www.sueddeutsche.de/politik/spionage-in-deutschland-verfassungsschutz-beliefert-nsa-1.1770672>) (in German). *Süddeutsche Zeitung*. Retrieved 18 December 2013.
14. ^{*a*} Kjetil Malkenes Hovland. "Norway Monitored Phone Traffic and Shared Data With NSA" (<http://online.wsj.com/news/articles/SB10001424052702303985504579207500439573552>). *The Wall Street Journal*. Retrieved 18 December 2013.
15. ^{*a*} "USA must not persecute whistleblower Edward Snowden" (<http://www.amnesty.org/en/news/usa-must-not-persecute-whistleblower-edward-snowden-2013-07-02>). Amnesty International. Retrieved August 16, 2013.
16. ^{*a*} "US: Statement on Protection of Whistleblowers in Security Sector" (<http://www.hrw.org/news/2013/06/18/us-statement-protection-whistleblowers-security-sector>). Human Rights Watch. Retrieved August 16, 2013.
17. ^{*a*} Transparency International Germany. "Transparency International Germany: Whistleblower Prize 2013 for Edward Snowden" (http://www.transparency.org/news/pressrelease/transparency_international_germany_whistleblower_prize_2013_for_edward_snow). Transparency International. Retrieved August 16, 2013.
18. ^{*a*} "US needs to protect whistleblowers and journalists" (<http://www.indexoncensorship.org/2013/06/us-needs-to-protect-whistleblowers-and-journalists/>). Index on Censorship. Retrieved August 16, 2013.
19. ^{*a*} U.S. vs. Edward J. Snowden criminal complaint (<http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/>). *The Washington Post*.
20. ^{*a*} "Leaker Files for Asylum to Remain in Russia" (<http://www.nytimes.com/2013/07/17/world/europe/snowden-submits-application-for-asylum-in-russia.html>). The New York Times. July 16, 2013. Retrieved December 16, 2013.
21. ^{*a*} "Snowden Asylum Hits U.S.-Russia Relations" (<http://online.wsj.com/article/SB10001424127887323681904578641610474568782.html>). The Wall Street Journal. August 1, 2013. Retrieved December 16, 2013.
22. ^{*a*} ".S. 'Extremely Disappointed' At Russia's Asylum For Snowden" (<http://www.npr.org/blogs/thetwo-way/2013/08/01/207831950/snowden-has-left-moscows-airport-as-russia-grants-asylum>). NPR. August 1, 2013. Retrieved December 16, 2013.
23. ^{*a*} Henderson. "Obama To Leno: 'There Is No Spying On Americans'" (<http://m.npr.org/news/U.S./209692380>). NPR. Retrieved August 16, 2013.
24. ^{*a*} Francis Elliott. "Cameron hints at action to stop security leaks" (<http://www.thetimes.co.uk/tto/news/politics/article3906802.ece>). *The Times*. Retrieved November 13, 2013.

25. ^a RAPHAEL SATTER. "UK Pursuing Criminal Investigation Into NSA Leaks" (<http://abcnews.go.com/International/wireStory/uk-pursuing-criminal-investigation-nsa-leaks-20867504>). ABC News. Retrieved November 13, 2013.
26. ^a "Only 1% of Snowden files published - Guardian editor" (<http://www.bbc.co.uk/news/uk-25205846>). BBC. December 3, 2013. Retrieved December 29, 2013.
27. ^{a b} Transcript Of President Obama's Speech On NSA Reforms (<http://www.npr.org/blogs/itsallpolitics/2014/01/17/263480199/transcript-of-president-obamas-speech-on-nsa-reforms>) *NPR* 17 January 2014
28. ^{a b} Sean Wilentz (19 January 2014), Would You Feel Differently About Snowden, Greenwald, and Assange If You Knew What They Really Thought? (<http://www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe>) *The New Republic*
29. ^a Barton Gellman (24 December 2013). "Edward Snowden, after months of NSA revelations, says his mission's accomplished" (http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html). *The Washington Post*. Retrieved 25 December 2013. "Taken together, the revelations have brought to light a global surveillance system that cast off many of its historical restraints after the attacks of Sept. 11, 2001. Secret legal authorities empowered the NSA to sweep in the telephone, Internet and location records of whole populations."
30. ^{a b} "Microsoft helped NSA, FBI access user info: Guardian" (<http://www.reuters.com/article/2013/07/11/us-usa-cybersecurity-microsoft-idUSBRE96A11R20130711>). Reuters. Jul 11, 2013. Retrieved 25 December 2013.
31. ^a Andy Greenberg (6/05/2013). "NSA's Verizon Spying Order Specifically Targeted Americans, Not Foreigners" (<http://www.forbes.com/sites/andygreenberg/2013/06/05/nsas-verizon-spying-order-specifically-targeted-americans-not-foreigners/>). Forbes. Retrieved 25 December 2013. "In a top secret order obtained by the Guardian newspaper and published Wednesday evening, the FBI on the NSA's behalf demanded that Verizon turn over all metadata for phone records originating in the United States for the three months beginning in late April and ending on the 19th of July."
32. ^a "Report: NSA and CIA collaborate on drone strikes" (<http://bigstory.ap.org/article/report-nsa-and-cia-collaborate-drone-strikes>). *Associated Press*. Oct 17, 2013. Retrieved 25 December 2013.
33. ^a Doug Gross (December 10, 2013). "Leak: Government spies snooped in 'Warcraft,' other games" (<http://edition.cnn.com/2013/12/09/tech/web/nsa-spying-video-games/>). *CNN*. Retrieved 25 December 2013.
34. ^a Craig Timberg and Barton Gellman. "NSA paying U.S. companies for access to communications networks" (http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html). *The Washington Post*. Retrieved 25 December 2013.
35. ^a Michael Winter (August 23, 2013). "NSA reimbursed tech firms millions for data" (<http://www.usatoday.com/story/news/nation/2013/08/23/nsa-paid-internet-firms-surveillance-prism/2693701/>). *USA Today*. Retrieved 25 December 2013.
36. ^a Brian Fung. "The NSA paid Silicon Valley millions to spy on taxpayers" (<http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/23/the-nsa-paid-google-and-facebook-millions-to-spy-on-taxpayers/>). *The Washington Post*. Retrieved 25 December 2013.
37. ^a Rob Williams (2 August 2013). "Americans pay GCHQ £100m to spy for them, leaked NSA papers from Edward Snowden claim" (<http://www.independent.co.uk/news/uk/home-news/americans-pay-gchq-100m-to-spy-for-them-leaked-nsa-papers-from-edward-snowden-claim-8743775.html>). *The Independent*. Retrieved 25 December 2013.
38. ^a Kiran Stacey (August 1, 2013). "US paid GCHQ £100m for UK intelligence, say leaked documents" (<http://www.ft.com/intl/cms/s/0/2013e09a-fac8-11e2-a7aa-00144feabdc0.html>). *Financial Times*. Retrieved 25 December 2013.
39. ^a "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_redaction&ns_mchannel=editors_picks&ns_source=google_actualite&ns_linkname=ameriques.20131130-espionnage-services-secrets-francais-precieux-partenaires-nsa-americaine&ns_fee=0) (in French). Radio France Internationale. Retrieved 30 November 2013.
40. ^a "SPIEGEL Reveals Cooperation Between NSA and German BND" (<http://www.spiegel.de/international/world/spiegel-reveals-cooperation-between-nsa-and-german-bnd-a-909954.html>). *Der Spiegel*. July 8, 2013. Retrieved 25 December 2013.

41. ^{a b} Ball, James (20 November 2013). "US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data" (<http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data>). *The Guardian*. Retrieved 21 November 2013.
42. ^a Philip Dorling (September 12, 2013). "US shares raw intelligence on Australians with Israel" (<http://www.smh.com.au/national/us-shares-raw-intelligence-on-australians-with-israel-20130912-2tllm.html>). *The Sydney Morning Herald*. Retrieved 25 December 2013.
43. ^a Ewen MacAskill, James Ball and Katharine Murphy (2 December 2013). "Revealed: Australian spy agency offered to share data about ordinary citizens" (<http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens>). *The Guardian*. Retrieved 25 December 2013.
44. ^{a b c d} David E.Sanger and Thom Shanker (14 January 2014). "N.S.A. Devises Radio Pathway Into Computers" (<http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?hp>). *The New York Times*. Retrieved 15 January 2014.
45. ^a Philip Dorling (June 13, 2013). "Australia gets 'deluge' of US secret data, prompting a new data facility" (<http://www.smh.com.au/it-pro/government-it/australia-gets-deluge-of-us-secret-data-prompting-a-new-data-facility-20130612-2o4kf.html>). *The Sydney Morning Herald*. Retrieved 22 December 2013.
46. ^a Nick Hopkins (7 June 2013). "UK gathering secret intelligence via covert NSA operation" (<http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>). *The Guardian*. Retrieved 22 December 2013.
47. ^a Olmer, Bart. "Ook AIVD bespiedt internetter" (http://www.telegraaf.nl/binnenland/21638965/_Ook_AIVD_bespiedt_internetter_.html) (in Dutch). *De Telegraaf*. Retrieved September 10, 2013. "Niet alleen Amerikaanse inlichtingendiensten monitoren internetters wereldwijd. Ook Nederlandse geheime diensten krijgen informatie uit het omstreden surveillanceprogramma 'Prism'."
48. ^{a b c} Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe (July 11, 2013). "Revealed: how Microsoft handed the NSA access to encrypted messages" (<http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data>). *The Guardian*. Retrieved July 11, 2013.
49. ^a Brandon Griggs (July 13, 2013). "Report: Microsoft collaborated closely with NSA" (<http://edition.cnn.com/2013/07/12/tech/web/microsoft-nsa-snooping/>). CNN. Retrieved 25 December 2013. "And Microsoft also worked with the FBI this year to give the NSA easier access to its cloud storage service SkyDrive"
50. ^{a b c} René Pfister, Laura Poitras, Marcel Rosenbach, Jörg Schindler and Holger Stark. "German Intelligence Worked Closely with NSA on Data Surveillance" (<http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html>). *Der Spiegel*. Retrieved 22 December 2013.
51. ^a Gunnar Rensfeldt. "FRA has access to controversial surveillance system" (<http://www.svt.se/ug/fra-has-access-to-controversial-surveillance-system>). Sveriges Television. Retrieved 12 December 2013.
52. ^{a b c d} Gunnar Rensfeldt. "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.
53. ^a Nick Hopkins and Julian Borger (1 August 2013). "Exclusive: NSA pays £100m in secret funding for GCHQ" (<http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>). *The Guardian*. Retrieved 22 December 2013.
54. ^a Rob Williams (2 August 2013). "Americans pay GCHQ £100m to spy for them, leaked NSA papers from Edward Snowden claim" (<http://www.independent.co.uk/news/uk/home-news/americans-pay-gchq-100m-to-spy-for-them-leaked-nsa-papers-from-edward-snowden-claim-8743775.html>). *The Independent*. Retrieved 31 December 2013.
55. ^{a b c d e f g h i j k l m n} James Ball, Luke Harding and Juliette Garside. "BT and Vodafone among telecoms companies passing details to GCHQ" (<http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq>). *The Guardian*. Retrieved 22 December 2013.
56. ^a Gellman, Barton; Soltani, Ashkan; Peterson, Andrea (November 4, 2013). "How we know the NSA had access to internal Google and Yahoo cloud data" (<http://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 November 5, 2013.
57. ^a Matthias Gebauer, Hubert Gude, Veit Medick, Jörg Schindler and 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.

58. [^] Philip Dorling (October 31, 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 23 December 2013.
59. [^] ^a ^b ^c ^d "Photo Gallery: Spies in the Embassy" (<http://www.spiegel.de/fotostrecke/photo-gallery-spies-in-the-embassy-fotostrecke-103079-5.html>). *Der Spiegel*. Retrieved 22 December 2013.
60. [^] Colin Freeze. "Canadian embassies eavesdrop, leak says" (<http://www.theglobeandmail.com/news/world/canada-involved-in-us-spying-efforts-abroad-leaked-document-says/article15133508/>). *The Globe and Mail*. Retrieved 23 December 2013.
61. [^] ^a ^b Duncan Campbell , Cahal Milmo , Kim Sengupta , Nigel Morris , Tony Patterson (5 November 2013). "Revealed: Britain's 'secret listening post in the heart of Berlin'" (<http://www.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html>). *The Independent*. Retrieved 22 December 2013.
62. [^] Duncan Campbell and Cahal Milmo (5 November 2013). "Exclusive: RAF Croughton base 'sent secrets from Merkel's phone straight to the CIA'" (<http://www.independent.co.uk/news/uk/politics/exclusive-raf-croughton-base-sent-secrets-from-merkels-phone-straight-to-the-cia-8923401.html>). *The Independent*. Retrieved 25 December 2013.
63. [^] ^a ^b ^c ^d 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.
64. [^] ^a ^b ^c "Espionnage : la France aurait collaboré avec la NSA" (<http://www.leparisien.fr/politique/espionnage-la-france-aurait-collabore-avec-la-nsa-29-10-2013-3268865.php>). *Le Parisien*. 2013-10-29. Retrieved 30 December 2013.
65. [^] "U.S. Electronic Espionage: A Memoir". *Ramparts*. August 1972. pp. 35–50. "The SIGINT community was defined by a TOP SECRET treaty signed in 1947. It was called the UKUSA treaty. The National Security Agency signed for the U.S. and became what's called First Party to the Treaty."
66. [^] Campbell, Duncan (1988-08-12). "Somebody's Listening" (<http://web.archive.org/web/20130420093650/http://duncan.gn.apc.org/echelon-dc.htm>). *New Statesman*. Archived from the original (<http://duncan.gn.apc.org/echelon-dc.htm>) on 2013-04-20. "The Congressional officials were first told of the Thurmond interception by a former employee of the Lockheed Space and Missiles Corporation, Margaret Newsham, who now lives in Sunnyvale, California."
67. [^] "Shayler: Whistleblower or traitor?" (http://news.bbc.co.uk/2/hi/talking_point/658129.stm). BBC. 3 March 2000. Retrieved 28 December 2013.
68. [^] JOSEPH FINDER (April 29, 2001). "Bugging the World" (<http://www.nytimes.com/books/01/04/29/reviews/010429.29findert.html>). *The New York Times*. Retrieved 28 December 2013.
69. [^] "NSA Whistleblowers William (Bill) Binney and J. Kirk Wiebe" (<http://www.whistleblower.org/program-areas/homeland-security-a-human-rights/surveillance/nsa-whistleblowers-bill-binney-a-j-kirk-wiebe>). Government Accountability Project.
70. [^] "Interview: Whistleblower Katharine Gun" (http://news.bbc.co.uk/2/hi/uk_news/politics/3659310.stm). BBC. 27 November 2003. Retrieved 28 December 2013.
71. [^] "UK 'spied on UN's Kofi Annan'" (http://news.bbc.co.uk/2/hi/uk_news/politics/3488548.stm). BBC. 26 February 2004. Retrieved 28 December 2013.
72. [^] JAMES RISEN and ERIC LICHTBLAU (December 16, 2005). "Bush Lets U.S. Spy on Callers Without Courts" (<http://www.nytimes.com/2005/12/16/politics/16program.html>). *The New York Times*.
73. [^] Leslie Cauley (5/11/2006). "NSA has massive database of Americans' phone calls" (http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm). *USA Today*.
74. [^] "Wiretap Whistle-Blower's Account" (<http://www.wired.com/science/discoveries/news/2006/04/70621>). *Wired (magazine)*. April 6, 2006. Retrieved 28 December 2013.
75. [^] Brian Ross (10 January 2006). "NSA Whistleblower Alleges Illegal Spying" (<http://abcnews.go.com/WNT/Investigation/story?id=1491889>). ABC News. Retrieved 28 December 2013.
76. [^] Ellen Nakashima (July 14, 2010). "Former NSA executive Thomas A. Drake may pay high price for media leak" (<http://www.washingtonpost.com/wp-dyn/content/article/2010/07/13/AR2010071305992.html>). *The Washington Post*. Retrieved 28 December 2013.

77. [^] "Wikileaks disclosure shines light on Big Brother" (<http://www.cbsnews.com/news/wikileaks-disclosure-shines-light-on-big-brother/>). CBS News. December 1, 2011.
78. [^] Michael Hastings (28 February 2012). "Exclusive: Homeland Security Kept Tabs on Occupy Wall Street" (<http://www.rollingstone.com/politics/blogs/national-affairs/exclusive-homeland-security-kept-tabs-on-occupy-wall-street-20120228>). Rolling Stone. Retrieved 5 January 2014.
79. [^] ^a ^b "How Edward Snowden led journalist and film-maker to reveal NSA secrets" (<http://www.theguardian.com/world/2013/aug/19/edward-snowden-nsa-secrets-glenn-greenwald-laura-poitras>). *The Guardian*. Retrieved August 20, 2013.
80. [^] ^a ^b Mark Hosenball (August 15, 2013), Snowden downloaded NSA secrets while working for Dell, sources say (<http://www.reuters.com/article/2013/08/15/us-usa-security-snowden-dell-idUSBRE97E17P20130815>) *Reuters*
81. [^] ^a ^b Peter Maass (August 18, 2013), "How Laura Poitras Helped Snowden Spill His Secrets" (<http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html>) *The New York Times*
82. [^] Carmon, Irin (June 10, 2013). "How we broke the NSA story" (http://www.salon.com/2013/06/10/qa_with_laura_poitras_the_woman_behind_the_nsa_scoops/singleton/). *Salon*. Retrieved June 11, 2013.
83. [^] Greenwald, Glenn; MacAskill, Ewen; Poitras, Laura (June 9, 2013). "Edward Snowden: the whistleblower behind the NSA surveillance revelations" (<http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>). *The Guardian* (London). Retrieved June 9, 2013.
84. [^] Smith, Matt; Pearson, Michael (June 10, 2013). "NSA leaker holed up in Hong Kong hotel, running low on cash" (<http://edition.cnn.com/2013/06/10/politics/nsa-leak/index.html>). CNN. Retrieved June 10, 2013.
85. [^] Everything We Learned From Edward Snowden in 2013 - NationalJournal.com (<http://www.nationaljournal.com/defense/everything-we-learned-from-edward-snowden-in-2013-20131231>)
86. [^] ^a ^b Glenn Greenwald (June 6, 2013). "NSA collecting phone records of millions of Verizon customers daily" (<http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order>). *The Guardian*. Retrieved September 16, 2013.
87. [^] "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program" (http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers). *The Washington Post*. Retrieved August 20, 2013.
88. [^] Laura Poitras, Marcel Rosenbach, Fidelius Schmid and Holger Stark (June 29, 2013). "NSA Spied on European Union Offices" (<http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html>). *Der Spiegel*.
89. [^] Laura Poitras, Marcel Rosenbach and Holger Stark. "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.html>). *Der Spiegel*.
90. [^] EXCLUSIVE: US hacks Chinese mobile phone companies (<http://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden>), *South China Morning Post*
91. [^] NSA targeted China's Tsinghua University in hacking attacks (<http://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking>), *South China Morning Post*
92. [^] Lam, Lana (June 23, 2013). "US hacked Pacnet, Asia Pacific fibre-optic network operator, in 2009" (<http://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator>). *South China Morning Post* (Hong Kong). Retrieved June 25, 2013.
93. [^] Laura Poitras, Marcel Rosenbach und Holger Stark. "Geheimdokumente: NSA überwacht 500 Millionen Verbindungen in Deutschland" (<http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html>). *Der Spiegel* (in German). Retrieved June 30, 2013.
94. [^] MacAskill, Ewen; Borger, Julian (June 30, 2013). "New NSA leaks show how US is bugging its European allies" (<http://www.guardian.co.uk/world/2013/jun/30/nsa-leaks-us-bugging-european-allies>). *The Guardian* (London).
95. [^] MacAskill, Ewen; Davies, Nick; Hopkins, Nick; Borger, Julian; Ball, James (June 17, 2013). "GCHQ intercepted foreign politicians' communications at G20 summits" (<http://www.guardian.co.uk/uk/2013/jun/16/gchq-intercepted-communications-g20-summits>). *The Guardian* (London).
96. [^] MacAskill, Ewen; Borger, Julian; Hopkins, Nick; Davies, Nick; Ball, James (June 21, 2013). "GCHQ taps fiber-optic cables for secret access to world's communications" (<http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>). *The Guardian*.
97. [^] ^a ^b Ewen MacAskill; Julian Borger; Nick Hopkins; Nick Davies; James Ball (21 June 2013). "GCHQ taps fibre-optic cables for secret access to world's communications" (<http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>). *The Guardian*. Retrieved 21 June 2013.

98. ^ Philip Bump (21 June 2013). "The UK Tempora Program Captures Vast Amounts of Data – and Shares with NSA" (<http://www.theatlanticwire.com/national/2013/06/uk-tempora-program/66490/>). The Atlantic Wire. Retrieved 23 June 2013.
99. ^ Glenn Greenwald and Spencer Ackerman (June 27, 2013). "NSA collected US email records in bulk for more than two years under Obama" (<http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama>). *The Guardian*. Retrieved August 1, 2013.
100. ^ Glenn Greenwald and Spencer Ackerman (June 27, 2013). "How the NSA is still harvesting your online data" (<http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection>). *The Guardian*. Retrieved August 1, 2013.
101. ^ Glenn Greenwald and Ewen MacAskill (11 June 2013). "Boundless Informant: the NSA's secret tool to track global surveillance data" (<http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>). *The Guardian*. Retrieved 1 January 2014.
102. ^ Laura Poitras, Marcel Rosenbach and Holger Stark. "Partner and Target: NSA Snoops on 500 Million German Data Connections" (<http://www.spiegel.de/international/germany/nsa-spies-on-500-million-german-data-connections-a-908648.html>). *Der Spiegel*. Retrieved 1 January 2014.
103. ^ Hubert Gude, Laura Poitras and Marcel Rosenbach. "German Intelligence Sends Massive Amounts of Data to the NSA" (<http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html>). *Der Spiegel*. Retrieved 1 January 2014.
104. ^ EUA espionaram milhões de e-mails e ligações de brasileiros (<http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>), *O Globo*, July 6, 2013. Retrieved July 8, 2013.
105. ^ The NSA's mass and indiscriminate spying on Brazilians (<http://www.guardian.co.uk/commentisfree/2013/jul/07/nsa-brazilians-globo-spying>), Glenn Greenwald, *The Guardian*, July 7, 2013. Retrieved July 8, 2013.
106. ^ EUA expandem o aparato de vigilância continuamente (<http://oglobo.globo.com/mundo/eua-expandem-aparato-de-vigilancia-continuamente-8941149>), *O Globo*, July 6, 2013. Retrieved July 8, 2013.
107. ^ ^a ^b ^c ^d ^e ^f ^g Philip Dorling (July 8, 2013). "Snowden reveals Australia's links to US spy web" (<http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html>). *The Sydney Morning Herald*. Retrieved July 8, 2013.
108. ^ "Interview with Whistleblower Edward Snowden on Global Spying" (<http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html>). *Der Spiegel*. July 8, 2013.
109. ^ "Edward Snowden Accuses Germany of Aiding NSA in Spying Efforts" (<http://www.spiegel.de/international/world/edward-snowden-accuses-germany-of-aiding-nsa-in-spying-efforts-a-909847.html>). *Der Spiegel*. July 7, 2013.
110. ^ '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 July 21, 2013.
111. ^ Geiger, Friedrich (August 3, 2013). "German Intelligence Agency Providing NSA With Metadata – Report" (<http://online.wsj.com/article/BT-CO-20130803-700914.html>). *The Wall Street Journal*. Retrieved August 3, 2013.
112. ^ ^a ^b ^c "Key Partners': Secret Links Between Germany and the NSA" (<http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355-2.html>). *Der Spiegel*. July 22, 2013. Retrieved 13 January 2014.
113. ^ ^a ^b Matthias Gebauer. "Prism in Afghanistan: Conflicting Accounts By German Government" (<http://www.spiegel.de/international/germany/a-911952.html>). *Der Spiegel*.
114. ^ Greenwald, Glenn (July 31, 2013). "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'" (<http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>). *The Guardian*. Retrieved August 1, 2013.
115. ^ Nakashima, Ellen (July 31, 2013). "Newly declassified documents on phone records program released" (http://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 August 4, 2013.
116. ^ Charlie Savage and David E. Sanger (July 31, 2013). "Senate Panel Presses N.S.A. on Phone Logs" (http://www.nytimes.com/2013/08/01/us/nsa-surveillance.html?pagewanted=all&_r=0). *The New York Times*. Retrieved August 4, 2013.
117. ^ Angwin, Julia (December 13, 2012). "U.S. Terrorism Agency to Tap a Vast Database of Citizens" (http://online.wsj.com/article/SB1000142412788732410820457902522244858490.html?mod=WSJEurope_hpp_LEFTTopStories). *The Wall Street Journal*. Retrieved August 21, 2013.

118. ^ Iain Thomson (July 8, 2013). "Snowden: US and Israel *did* create Stuxnet attack code" (http://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet/). *The Register*. Retrieved July 8, 2013.
119. ^ Révélations sur le Big Brother français (http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441631_3224.html) (2) (<http://democratie-reelle-nimes.over-blog.com/article-revelations-sur-le-big-brother-fran-ais-la-totalite-de-nos-communications-sont-espionnees-mails-118897483.html>), *Le Monde*, July 4, 2013. Retrieved July 5, 2013.
120. ^ France 'runs vast electronic spying operation using NSA-style methods' (<http://www.guardian.co.uk/world/2013/jul/04/france-electronic-spying-operation-nsa>), *The Guardian*, July 4, 2013. Retrieved July 5, 2013.
121. ^ ^a ^b ^c ^d ^e ^f ^g John Goetz and Frederik Obermaier. "Snowden enthüllt Namen der spähenden Telekommunikationsfirmen" (<http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthueellt-namen-der-spahenden-telekommunikationsfirmen-1.1736791>). *Süddeutsche Zeitung* (in German). Retrieved August 2, 2013. "In den internen Papieren des GCHQ aus dem Jahr 2009 stehen sie nun aufgelistet: Verizon Business, Codename: Dacron, British Telecommunications (codenamed "Remedy"), Vodafone Cable ("Gerontic"), Global Crossing ("Pinnacle"), Level 3 (codenamed "Little"), Viatel ("Vitreous") und Interoute ("Streetcar")."
122. ^ ^a ^b ^c ^d John Goetz, Hans Leyendecker and Frederik Obermaier (August 28, 2013). "British Officials Have Far-Reaching Access To Internet And Telephone Communications" (<http://international.sueddeutsche.de/post/59603415442/british-officials-have-far-reaching-access-to-internet>). *Süddeutsche Zeitung*. Retrieved August 28, 2013.
123. ^ Dorling, Philip. "Australian spies in global deal to tap undersea cables" (<http://www.smh.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html>). *The Sydney Morning Herald*. Retrieved August 29, 2013.
124. ^ ^a ^b "U.S. spy agency bugged U.N. headquarters: Germany's Spiegel" (<http://www.reuters.com/article/2013/08/25/us-usa-security-nsa-un-idUSBRE9700DD20130825>). Reuters. Aug 25, 2013. Retrieved 12 January 2014.
125. ^ ^a ^b "US-Geheimdienst hörte Zentrale der Vereinten Nationen ab" (<http://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html>). *Der Spiegel* (in German). Retrieved August 25, 2013.
126. ^ Savage, Charlie (August 8, 2013). "N.S.A. Said to Search Content of Messages to and From U.S." (<http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all>). *The New York Times*. Retrieved September 30, 2013.
127. ^ "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>). Der Spiegel. August 31, 2013. Retrieved 1 January 2014.
128. ^ Siobhan Gorman and Jennifer Valentiono-Devries (August 20, 2013). "New Details Show Broader NSA Surveillance Reach – Programs Cover 75% of Nation's Traffic, Can Snare Emails" (http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html?mod=WSJEurope_hpp_LEFTTopStories). *The Wall Street Journal*. Retrieved August 21, 2013.
129. ^ "Graphic: How the NSA Scours Internet Traffic in the U.S." (http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html?mod=WSJEurope_hpp_LEFTTopStories#project%3DNSA0820%26articleTabs%3Dinteractive). *The Wall Street Journal*. August 20, 2013. Retrieved August 21, 2013.
130. ^ Jennifer Valentiono-Devries and Siobhan Gorman (August 20, 2013). "What You Need to Know on New Details of NSA Spying" (http://online.wsj.com/article/SB1000142412788732410820457902522244858490.html?mod=WSJEurope_hpp_LEFTTopStories). *The Wall Street Journal*. Retrieved August 21, 2013.
131. ^ Jennifer Valentino-Devries and Danny Yadron (August 1, 2013). "FBI Taps Hacker Tactics to Spy on Suspects" (<http://online.wsj.com/article/SB10001424127887323997004578641993388259674.html>). *The Wall Street Journal*. Retrieved October 9, 2013.
132. ^ Jennifer Valentino-DeVries and Danny Yadron (August 1, 2013). "How the FBI Hacks Criminal Suspects" (<http://blogs.wsj.com/digits/2013/08/01/how-the-fbi-hacks-criminal-suspects/>). *The Wall Street Journal*. Retrieved October 9, 2013.
133. ^ "NSA report on privacy violations in the first quarter of 2012" (<http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/>). *The Washington Post*. August 16, 2013. Retrieved August 16, 2013.
134. ^ Barton Gellman and Matt DeLong (August 15, 2013). "What to say, and not to say, to 'our overseers'" (<http://apps.washingtonpost.com/g/page/national/what-to-say-and-not-to-say-to-our-overseers/390/#more>). *The Washington Post*. Retrieved August 25, 2013.

135. ^ Barton Gellman and Matt DeLong (August 15, 2013). "First direct evidence of illegal surveillance found by the FISA court" (<http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393/>). *The Washington Post*. Retrieved August 25, 2013.
136. ^ Gellmann, Barton (August 16, 2013). "NSA broke privacy rules thousands of times per year, audit finds" (http://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). *The Washington Post*. Retrieved August 24, 2013.
137. ^ Nakashima, Ellen (August 16, 2013). "Lawmakers, privacy advocates call for reforms at NSA" (http://www.washingtonpost.com/world/national-security/lawmakers-privacy-advocates-call-for-reforms-at-nsa/2013/08/16/7cccb772-0692-11e3-a07f-49ddc7417125_story.html). *The Washington Post*. Retrieved August 25, 2013.
138. ^ Gellmann, Barton (August 16, 2013). "NSA statements to The Post" (http://www.washingtonpost.com/world/national-security/nsa-statements-to-the-post/2013/08/15/f40dd2c4-05d6-11e3-a07f-49ddc7417125_story.html). *The Washington Post*. Retrieved August 25, 2013.
139. ^ Barton Gellman and Matt DeLong (August 15, 2013). "What's a 'violation'?" (<http://apps.washingtonpost.com/g/page/national/whats-a-violation/391/>). *The Washington Post*. Retrieved August 25, 2013.
140. ^ Leonnig, Carol D. (August 16, 2013). "Court: Ability to police U.S. spying program limited" (http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html). *The Washington Post*. Retrieved August 25, 2013.
141. ^ Nakashima, Ellen (August 21, 2013). "NSA gathered thousands of Americans' e-mails before court ordered it to revise its tactics" (http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html). *The Washington Post*. Retrieved September 16, 2013.
142. ^ "FISA court ruling on illegal NSA e-mail collection program" (<http://apps.washingtonpost.com/g/page/national/fisa-court-documents-on-illegal-nsa-e-mail-collection-program/409/>). *The Washington Post*. August 21, 2013. Retrieved September 16, 2013.
143. ^ Barton Gellman and Matt DeLong (August 15, 2013). "First direct evidence of illegal surveillance found by the FISA court" (<http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393/>). *The Washington Post*. Retrieved September 16, 2013.
144. ^ Charlie Savage and Scott Shane (August 21, 2013). "Secret Court Rebuked N.S.A. on Surveillance" (http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?_r=3&&pagewanted=all). *The New York Times*. Retrieved September 16, 2013.
145. ^ Mark Hosenball and Tabassum Zakaria (August 22, 2013). "NSA collected 56,000 emails by Americans a year: documents" (<http://www.nbcnews.com/technology/nsa-collected-56-000-emails-americans-year-documents-6C10975688>). *Reuters*. NBC News. Retrieved September 16, 2013.
146. ^ ^a ^b Craig Timberg and Barton Gellman (August 30, 2013). "NSA paying U.S. companies for access to communications networks" (http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html). *The Washington Post*. Retrieved August 31, 2013.
147. ^ Wallsten, Peter (August 17, 2013). "House panel withheld document on NSA surveillance program from members" (http://www.washingtonpost.com/politics/house-panel-withheld-document-on-nsa-surveillance-program-from-members/2013/08/16/944e728e-0672-11e3-9259-e2aaf5a5f84_story.html). *The Washington Post*. Retrieved August 25, 2013.
148. ^ Weich, Ronald. "Report of the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization" (http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf). *Office of the Assistant Attorney General*. Director of National Intelligence. Retrieved August 25, 2013.
149. ^ James Ball, Luke Harding and Juliette Garside (August 1, 2013). "Exclusive: NSA pays £100m in secret funding for GCHQ" (<http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>). Retrieved August 2, 2013.
150. ^ James Ball and Spencer Ackerman (August 9, 2013). "NSA loophole allows warrantless search for US citizens' emails and phone calls – Exclusive: Spy agency has secret backdoor permission to search databases for individual Americans' communications" (<http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls>). *The Guardian*. Retrieved August 12, 2013.

151. ^ Farivar, Cyrus (August 10, 2013). "New leak: NSA can search US e-mail data but theoretically won't" (<http://arstechnica.com/tech-policy/2013/08/new-leak-nsa-can-search-us-e-mail-data-but-theoretically-isnt-allowed-to/>). *Ars Technica*. Retrieved August 13, 2013.
152. ^ Roberts, Dan (August 23, 2013). "US surveillance guidelines not updated for 30 years, privacy board finds – Privacy watchdog points out in letter to intelligence chiefs that rules designed to protect Americans are severely outdated" (<http://www.theguardian.com/world/2013/aug/23/us-surveillance-rules-30-years>). *The Guardian*. Retrieved August 24, 2013.
153. ^ Medine, David (August 22, 2013). "2013-08-22 Privacy and Civil Liberties Oversight Board letter to US Attorney General Eric Holder and Director of National Intelligence James Clapper" (<https://s3.amazonaws.com/s3.documentcloud.org/documents/778168/pcllob-guidelines-letter-1.pdf>). Privacy & Civil Liberties Oversight Board. Retrieved August 24, 2013.
154. ^ Strohm, Chris (August 24, 2013). "Lawmakers Probe Willful Abuses of Power by NSA Analysts" (<http://www.bloomberg.com/news/2013-08-23/nsa-analysts-intentionally-abused-spying-powers-multiple-times.html>). Bloomberg News. Retrieved August 24, 2013.
155. ^ Roberts, Dan (August 23, 2013). "NSA analysts deliberately broke rules to spy on Americans, agency reveals – Inspector general's admission undermines fresh insistences from president that breaches of privacy rules were inadvertent" (<http://www.theguardian.com/world/2013/aug/23/nsa-analysts-broke-rules-spy>). *The Guardian*. Retrieved August 24, 2013.
156. ^ Gorman, Siobhan (August 23, 2013). "NSA Officers Spy on Love Interests" (<http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/>). *The Wall Street Journal*. Retrieved August 24, 2013.
157. ^ MacAskill, Ewen (August 23, 2013). "NSA paid millions to cover Prism compliance costs for tech companies • Top-secret files show first evidence of financial relationship • Prism companies include Google and Yahoo, says NSA • Costs were incurred after 2011 Fisa court ruling" (<http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid>). *The Guardian*. Retrieved August 24, 2013.
158. ^ David Leppard and Chris Williams (May 3, 2009). "Jacqui Smith's secret plan to carry on snooping" (<http://www.timesonline.co.uk/tol/news/politics/article6211101.ece>). *The Sunday Times*. Retrieved May 3, 2009.
159. ^ Henry Porter. "GCHQ revelations: mastery of the internet will mean mastery of everyone" (<http://www.theguardian.com/commentisfree/2013/jun/21/gchq-mastery-internet-mastery-everyone>). *The Guardian*. Retrieved October 19, 2013.
160. ^ James Ball, Julian Borger and Glenn Greenwald (September 5, 2013). "US and UK spy agencies defeat privacy and security on the internet" (<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>). *The Guardian*. Retrieved September 5, 2013.
161. ^ Nicole Perlroth, Jeff Larson and Scott Shane (September 5, 2013). "N.S.A. Foils Much Internet Encryption" (http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0). *The New York Times*. Retrieved September 5, 2013.
162. ^ "Secret Documents Reveal N.S.A. Campaign Against Encryption" (<http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us>). *The New York Times*. September 5, 2013. Retrieved September 7, 2013.
163. ^ "Unlocking Private Communications" (<http://www.nytimes.com/interactive/2013/09/05/us/unlocking-private-communications.html?ref=us>). *The New York Times*. September 5, 2013. Retrieved September 7, 2013.
164. ^ Perlroth, Nicole, Larson, Jeff, and Shane, Scott (September 5, 2013). "The NSA's Secret Campaign to Crack, Undermine Internet Security" (<http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>). *ProPublica*.
165. ^ Nakashima, Ellen (September 6, 2013). "NSA has made strides in thwarting encryption used to protect Internet communication" (http://www.washingtonpost.com/world/national-security/nsa-has-made-strides-in-thwarting-encryption-used-to-protect-internet-communication/2013/09/05/0ec08efc-1669-11e3-a2ec-b47e45e6f8ef_story.html?hpid=z3). *The Washington Post*. Retrieved September 7, 2013.
166. ^ Guillaume Champeau. "Lustre : la France aurait coopéré avec la NSA" (<http://www.numerama.com/magazine/27347-lustre-la-france-aurait-coopere-avec-la-nsa.html>) (in French). Numerama. Retrieved 30 December 2013.
167. ^ ^a ^b "Espionnage : la France perd son Lustre" (<http://www.zdnet.fr/actualites/espionnage-la-france-perd-son-lustre-39795120.htm>) (in French). ZDNet. 28 Octobre 2013. Retrieved 30 December 2013.
168. ^ "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>). *Der Spiegel*. September 15, 2013. Retrieved September 24, 2013.

169. [^] "Brazil Angered Over Report N.S.A. Spied on President" (http://www.nytimes.com/2013/09/03/world/americas/brazil-angered-over-report-nsa-spied-on-president.html?_r=0). The New York Times. Retrieved September 16, 2013.
170. [^] "NSA Documents Show United States Spied Brazilian Oil Giant" (<http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html>). *Jornal da Globo Fantástico*. September 8, 2013. Retrieved September 24, 2013.
171. [^] James Risen and Laura Poitras (September 28, 2013). "N.S.A. Gathers Data on Social Connections of U.S. Citizens" (http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0&pagewanted=all). *The New York Times*. Retrieved September 30, 2013.
172. [^] "NSA and Israeli intelligence: memorandum of understanding – full document" (<http://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document>). *The Guardian*. September 11, 2013. Retrieved September 14, 2013.
173. [^] Barton Gellman. "Secret documents detail U.S. war in cyberspace" (<http://www.japantimes.co.jp/news/2013/08/31/world/secret-documents-detail-u-s-war-in-cyberspace>). *The Washington Post* (via *The Japan Times*). Retrieved September 2, 2013.
174. [^] Barton Gellman and Ellen Nakashima (August 31, 2013). "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show" (http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html). *The Washington Post*. Retrieved August 31, 2013.
175. [^] Konrad Lischka und Julia Stanek (August 31, 2013). "Cyber-Angriffe: USA infizieren Zehntausende Computer mit NSA-Trojanern" (<http://www.spiegel.de/netzwelt/web/genie-programm-usa-infizierten-zehntausende-rechner-a-919625.html>). *Der SPIEGEL* (in German). Retrieved August 31, 2013.
176. [^] Zetter, Kim (September 4, 2013). "NSA Laughs at PCs, Prefers Hacking Routers and Switches" (<http://www.wired.com/threatlevel/2013/09/nsa-router-hacking/>). *Wired.com*. Retrieved October 2, 2013.
177. ^{^ a b c d e} Laura Poitras, Marcel Rosenbach and 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>). *Der Spiegel*. Retrieved September 9, 2013.
178. ^{^ a b} Laura Poitras, Marcel Rosenbach, and Holger Stark. "Photo Gallery: Spying on Smartphones" (<http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201.html>). *Der Spiegel*. Retrieved September 9, 2013.
179. [^] Barton Gellman, Craig Timberg and Steven Rich (4 October 2013). "Secret NSA documents show campaign against Tor encrypted network" (http://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.
180. [^] Steven Rich and Matt DeLong (4 October 2013). "NSA slideshow on 'The TOR problem'" (<http://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/>). *The Washington Post*. Retrieved 19 November 2013.
181. [^] Lee, Timothy B. (4 October 2013). "Everything you need to know about the NSA and Tor in one FAQ" (<http://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.
182. [^] "NSA report on the Tor encrypted network" (<http://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.
183. [^] "GCHQ report on 'MULLENIZE' program to 'stain' anonymous electronic traffic" (<http://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.
184. [^] James Ball, Bruce Schneier and Glenn Greenwald (4 October 2013). "NSA and GCHQ target Tor network that protects anonymity of web users" (<http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption>). *The Guardian*. Retrieved 19 November 2013.
185. [^] Schneier, Bruce (4 October 2013). "Attacking Tor: how the NSA targets users' online anonymity" (<http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>). *The Guardian*. Retrieved 19 November 2013.
186. [^] "'Tor Stinks' presentation – read the full document" (<http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>). *The Guardian*. 4 October 2013. Retrieved 19 November 2013.
187. [^] "Tor: 'The king of high-secure, low-latency anonymity'" (<http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity>). *The Guardian*. 4 October 2013. Retrieved 19 November 2013.

188. ^ "Ministério de Minas e Energia está na mira de espões americanos e canadenses" (<http://g1.globo.com/fantastico/noticia/2013/10/ministerio-das-minas-e-energia-esta-na-mira-de-espoes-americanos-e-canadenses.html>). *O Globo*. October 6, 2013. Retrieved October 8, 2013.
189. ^ "Report: Canada spies targeted Brazil mine ministry" (<http://bigstory.ap.org/article/report-canada-spies-targeted-brazil-mine-ministry>). *Associated Press*. Associated Press. October 6, 2013. Retrieved October 8, 2013.
190. ^ Ockenden, Will (October 8, 2013). "Australia prepared briefing on US global internet spying program PRISM before Snowden revelations" (<http://www.abc.net.au/news/2013-10-08/australia-prepared-briefing-on-prism-spying-program/5004290>). ABC News (Australia). Retrieved October 8, 2013.
191. ^ "AG Department Prism FOI PDF" (<http://de.scribd.com/doc/174279481/ag-department-prism-foi-pdf>). ABC News Online. June 27, 2013. Retrieved October 8, 2013.
192. ^ Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark (October 20, 2013). "Fresh Leak on US Spying: NSA Accessed Mexican President's Email" (<http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html>). *Der Spiegel*. Retrieved October 22, 2013.
193. ^ "NSA-Spionage: Mexiko fordert Aufklärung über US-Bespitzelungen" (<http://www.spiegel.de/politik/ausland/nsa-spionage-mexiko-fordert-aufklaerung-ueber-us-bespitzelungen-a-928946.html>). *Der Spiegel* (in German). October 21, 2013. Retrieved October 22, 2013.
194. ^ Mark Mazzetti and David E. Sanger (October 30, 2013). "Tap on Merkel Provides Peek at Vast Spy Net" (<http://www.nytimes.com/2013/10/31/world/europe/tap-on-merkel-provides-peek-at-vast-spy-net.html?src=recg&pagewanted=all>). *The New York Times*. Retrieved November 1, 2013.
195. ^ Mark Landler and Michael S. Schmidt (October 30, 2013). "Spying Known at Top Levels, Officials Say" (<http://www.nytimes.com/2013/10/30/world/officials-say-white-house-knew-of-spying.html?src=recg&pagewanted=all>). *The New York Times*. Retrieved November 1, 2013.
196. ^ ^a ^b Ball, James (October 24, 2013). "NSA monitored calls of 35 world leaders after US official handed over contacts" (<http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>). *The Guardian*. Retrieved October 24, 2013.
197. ^ ^a ^b Siobhan Gorhan and Adam Entous (October 28, 2013). "Obama Unaware as U.S. Spied on World Leaders: Officials" (<http://online.wsj.com/news/articles/SB10001424052702304470504579162110180138036>). *The Wall Street Journal*. Retrieved October 28, 2013.
198. ^ Ball, James (October 25, 2013). "Leaked memos reveal GCHQ efforts to keep mass surveillance secret" (<http://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden>). *The Guardian*. Retrieved October 25, 2013.
199. ^ Nakashima, Ellen (October 2, 2013). "NSA had test project to collect data on Americans' cellphone locations, director says" (http://www.washingtonpost.com/world/national-security/nsa-had-test-project-to-collect-data-on-americans-cellphone-locations-director-says/2013/10/02/65076278-2b71-11e3-8ade-a1f23cda135e_story.html). *The Washington Post*. Retrieved October 18, 2013.
200. ^ Barton Gellman and Ashkan Soltani (October 30, 2013). "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say" (http://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 October 31, 2013.
201. ^ Barton Gellman, Todd Lindeman and Ashkan Soltani (October 30, 2013). "How the NSA is infiltrating private networks" (<http://apps.washingtonpost.com/g/page/national/the-nsa-is-hacking-private-networks/542/>). *The Washington Post*. Retrieved October 31, 2013.
202. ^ Barton Gellman and Matt DeLong (October 30, 2013). "How the NSA's MUSCULAR program collects too much data from Yahoo and Google" (<http://apps.washingtonpost.com/g/page/world/how-the-nas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/>). *The Washington Post*. Retrieved October 31, 2013.
203. ^ Peterson, Andrea (October 30, 2013). "PRISM already gave the NSA access to tech giants. Here's why it wanted more." (<http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/30/prism-already-gave-the-nsa-access-to-tech-giants-heres-why-it-wanted-more/>). *The Washington Post*. Retrieved October 31, 2013.

204. [^] Washington Post Staff (October 30, 2013). "NSA statement on Washington Post report on infiltration of Google, Yahoo data center links" (http://www.washingtonpost.com/world/national-security/nsa-statement-on-washington-post-report-on-infiltration-of-google-yahoo-data-center-links/2013/10/30/5c135254-41b4-11e3-a624-41d661b0bb78_story.html). *The Washington Post*. Retrieved October 31, 2013.
205. [^] Jacob Appelbaum, Holger Stark, Marcel Rosenbach and Jörg Schindler (October 23, 2013). "Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?" (<http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicious-us-tapped-her-mobile-phone-a-929642.html>). *Der Spiegel*. Retrieved October 25, 2013.
206. [^] Fischer, Sebastian (October 24, 2013). "Merkel's Phone: Spying Suspicions Put Obama in a Tight Spot" (<http://www.spiegel.de/international/world/suspicious-of-us-spying-on-merkel-phone-awkward-for-obama-a-929692.html>). *Der Spiegel*. Retrieved October 25, 2013.
207. [^] Charly Wilder and Rupert Neat (October 24). "'Out of Hand': Europe Furious Over US Spying Allegations" (<http://www.spiegel.de/international/world/angry-european-and-german-reactions-to-merkel-us-phone-spying-scandal-a-929725.html>). *Der Spiegel*. Retrieved October 25, 2013.
208. [^] Ian Traynor in Brussels, Philip Oltermann in Berlin, and Paul Lewis in Washington (October 24). "Angela Merkel's call to Obama: are you bugging my mobile phone?" (<http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german>). *The Guardian*. Retrieved October 25, 2013.
209. [^] Ball, James (October 25, 2013). "NSA monitored calls of 35 world leaders after US official handed over contacts" (<http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>). *The Guardian*. Retrieved October 25, 2013.
210. [^] Traynor, Ian (October 25, 2013). "Germany and France warn NSA spying fallout jeopardises fight against terror" (<http://www.theguardian.com/world/2013/oct/25/germany-france-nsa-spying-merkel-hollande-eu>). *The Guardian*. Retrieved October 25, 2013.
211. [^] ^a ^b Jacob Appelbaum, Nikolaus Blome, Hubert Gude, Ralf Neukirch, René Pfister, Laura Poitras, Marcel Rosenbach, Jörg Schindler, Gregor Peter Schmitz and Holger Stark. Translated from the German by Kristen Allen and Charly Wilder. (October 27, 2013). "Der Spiegel Cover Story: How NSA Spied on Merkel Cell Phone from Berlin Embassy - Embassy Espionage: The NSA's Secret Spy Hub in Berlin" (<http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>). *Der Spiegel*. Retrieved November 1, 2013.
212. [^] "NSA-Überwachung: Merkels Handy steht seit 2002 auf US-Abhörliste" (<http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html>). *Der Spiegel* (in German). October 26, 2012. Retrieved October 26, 2013.
213. [^] "U.S. monitored German Chancellor Angela Merkel's phone since 2002" (<http://www.dailymail.co.uk/news/article-2477593/U-S-monitored-German-Chancellor-Angela-Merkels-phone-2002.html>). *Daily Mail*. October 26, 2012. Retrieved October 26, 2013.
214. [^] Ofer Aderet (October 26, 2015). "Obama: Had I known NSA tapped Merkel's cell, I would have stopped it, German media reports" (<http://www.haaretz.com/news/world/1.554526>). *Haaretz*. Retrieved October 26, 2013.
215. [^] David E. Sanger and Mark Mazzetti (October 24, 2013). "Allegation of U.S. Spying on Merkel Puts Obama at Crossroads" (<http://www.nytimes.com/2013/10/25/world/europe/allegation-of-us-spying-on-merkel-puts-obama-at-crossroads.html>). *The New York Times*. Retrieved October 26, 2013.
216. [^] Ian Traynor and Paul Lewis (17 December 2013). "Merkel compared NSA to Stasi in heated encounter with Obama" (<http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama>). *The Guardian*. Retrieved 18 December 2013.
217. [^] "Germany hopes for details from Snowden on US spying" (<http://www.bbc.co.uk/news/world-europe-24770430>). *bbc.co.uk*. November 1, 2013. Retrieved November 1, 2013.
218. [^] "Photo Gallery: Spies in the Embassy 10/27/2013" (<http://www.spiegel.de/fotostrecke/photo-gallery-spies-in-the-embassy-fotostrecke-103079.html>). *Der Spiegel*. October 27, 2013. Retrieved November 1, 2013.
219. [^] ^a ^b Dorling, Philipp (October 31, 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 November 1, 2013.
220. [^] Konrad Lischka and Matthias Kremp (October 28, 2013). "NSA-Spähskandal: So funktionieren die Abhöranlagen in US-Botschaften" (<http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaehskandal-so-funktionieren-die-abhoeranlagen-in-us-botschaften-a-930392.html>). *Der Spiegel* (in German). Retrieved November 1, 2013.
221. [^] Perlez, Jane (October 31, 2013). "Australia Said to Play Part in N.S.A. Effort" (<http://www.nytimes.com/2013/11/01/world/asia/australia-participated-in-nsa-program-document-says.html?src=recg>). *The New York Times*. Retrieved November 1, 2013.

222. [^] Jacques Follorou and Glenn Greenwald (October 21, 2013). "France in the NSA's crosshair : phone networks under surveillance" (http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html). *Le Monde*. Retrieved October 22, 2013.
223. [^] Gearan, Anna (October 22, 2013). "Report that NSA collected French phone records causing diplomatic headache for U.S." (http://www.washingtonpost.com/world/national-security/report-that-nsa-collected-french-phone-records-causing-diplomatic-headache-for-us/2013/10/21/bfa74f22-3a76-11e3-a94f-b58017bfee6c_story.html). *The Washington Post*. Retrieved October 22, 2013.
224. [^] Adam Entous and Siobhan Gorman (October 29, 2013). "U.S. Says France, Spain Aided NSA Spying" (<http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502>). *The Wall Street Journal*. Retrieved October 29, 2013.
225. [^] Ellen Nakashima and Karen DeYoung (October 29, 2013). "NSA chief says NATO allies shared phone records with the U.S. spy agency" (http://www.washingtonpost.com/world/national-security/top-intelligence-officials-called-to-testify-on-nsa-surveillance-programs/2013/10/29/e9e9c250-40b7-11e3-a751-f032898f2dbc_story.html). *The Washington Post*. Retrieved October 30, 2013.
226. [^] "Espionnage de la NSA : tous les documents publiés par "Le Monde"" (http://www.lemonde.fr/technologies/article/2013/10/21/espionnage-de-la-nsa-tous-les-documents-publies-par-le-monde_3499986_651865.html). *Le Monde*. October 21, 2013. Retrieved October 22, 2013.
227. [^] Miguel González. "NSA revelations: Spain also a victim of US espionage" (http://elpais.com/elpais/2013/10/25/inenglish/1382703360_329586.html). *El Pais*. Retrieved 13 December 2013.
228. [^] Miguel González. "España eleva el tono de las quejas a EE UU por el espionaje masivo" (http://internacional.elpais.com/internacional/2013/10/27/actualidad/1382912344_420746.html) (in Spanish). *El Pais*. Retrieved 13 December 2013.
229. [^] Paul Hamilos. "Spain colluded in NSA spying on its citizens, Spanish newspaper reports" (<http://www.theguardian.com/world/2013/oct/30/spain-colluded-nsa-spying-citizens-spanish-el-mundo-us>). *The Guardian*. Retrieved 22 December 2013.
230. [^] Glenn Greenwald and 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.
231. [^] ^a ^b Shane, Scott (2013-11-02). "No Morsel Too Minuscule for All-Consuming N.S.A." (http://www.webcitation.org/query?url=http%3A%2F%2Fwww.nytimes.com%2F2013%2F11%2F03%2Fworld%2Fno-morsel-too-minuscule-for-all-consuming-nsa.html%3Fpagewanted%3D7%26_r%3D2%26pagewanted%3Dall&date=2013-11-25). *New York Times*. Archived from the original (http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=7&_r=2&pagewanted=all) on 2013-11-25. Retrieved 2013-11-25. "This "communications fingerprinting," as a document called it, is the key to what the N.S.A. does. It allows the agency's computers to scan the stream of international communications and pluck out messages tied to the supreme leader."
232. [^] Campbell, Duncan (November 5, 2013). "Revealed: Britain's 'secret listening post in the heart of Berlin'" (<http://www.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html>). *The Independent*. Retrieved November 5, 2013.
233. [^] ^a ^b Tony Paterson. "GCHQ used 'Quantum Insert' technique to set up fake LinkedIn pages and spy on mobile phone giants" (<http://www.independent.co.uk/news/uk/home-news/gchq-used-quantum-insert-technique-to-set-up-fake-linkedin-pagesand-spy-on-mobile-phone-giants-8931528.html>). *The Independent*. Retrieved November 10, 2013.
234. [^] ^a ^b Laura Poitras, Marcel Rosenbach and Holger Stark (November 17, 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>). *Der Spiegel*. Retrieved November 17, 2013.
235. [^] Indonesia recalls Canberra ambassador over Yudhoyono phone tapping attempt, Foreign minister demands explanation after documents reveal Australian agencies targeted phones of president and his wife (<http://www.theguardian.com/world/2013/nov/18/indonesia-recalls-ambassador-yudhoyono-phone-tapping-australia>) The Guardian 18 November 2013
236. [^] ^a ^b ^c ^d ^e ^f ^g ^h ⁱ 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.

237. ^{a b} JAMES RISEN and LAURA POITRAS (November 22, 2013). "N.S.A. Report Outlined Goals for More Power" (<http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html>). *The New York Times*. Retrieved 23 November 2013.
238. ^a "A Strategy for Surveillance Powers" (<http://www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html>). *The New York Times*. Retrieved 23 November 2013.
239. ^a Floor Boon, Steven Derix and Huib Modderkolk. "Document Snowden: Nederland al sinds 1946 doelwit van NSA" (<http://www.nrc.nl/nieuws/2013/11/23/nederland-sinds-1946-doelwit-van-nsa/>). *NRC Handelsblad* (in Dutch). Retrieved 23 November 2013.
240. ^{a b} Floor Boon, Steven Derix and Huib Modderkolk. "NSA infected 50,000 computer networks with malicious software" (<http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/>). *NRC Handelsblad*. Retrieved 23 November 2013.
241. ^a Ewen MacAskill, James Ball and Katharine Murphy. "Revealed: Australian spy agency offered to share data about ordinary citizens" (<http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens>). *The Guardian*. Retrieved 3 December 2013.
242. ^{a b} Barton Gellman and Ashkan Soltani (4 December 2013). "NSA tracking cellphone locations worldwide, Snowden documents show" (http://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.
243. ^a "How the NSA is tracking people right now" (<http://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.
244. ^a Ashkan Soltani and Matt DeLong (4 December 2013). "FASCIA: The NSA's huge trove of location records" (<http://apps.washingtonpost.com/g/page/world/what-is-fascia/637/>). *The Washington Post*. Retrieved 6 December 2013.
245. ^a "How the NSA uses cellphone tracking to find and 'develop' targets" (http://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.
246. ^a "Reporter explains NSA collection of cellphone data" (http://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.
247. ^a Peterson, Andrea (4 December 2013). "The NSA says it 'obviously' can track locations without a warrant. That's not so obvious." (<http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/04/the-nsa-says-it-obviously-can-track-locations-without-a-warrant-thats-not-so-obvious/>). *The Washington Post's The Switch*. Retrieved 6 December 2013.
248. ^a Lee, Timothy (4 December 2013). "The NSA could figure out how many Americans it's spying on. It just doesn't want to." (http://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.
249. ^a Ashkan Soltani and Barton Gellman (10 December 2013). "New documents show how the NSA infers relationships based on mobile location data" (<http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/>). *The Washington Post*. Retrieved 26 December 2013.
250. ^a Ashkan Soltani, Andrea Peterson and Barton Gellman (10 December 2013). "NSA uses Google cookies to pinpoint targets for hacking" (<http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/>). *The Washington Post*. Retrieved 28 January 2014.
251. ^a Ashkan Soltani and Matt DeLong (10 December 2013). "NSA signal-surveillance success stories" (<http://apps.washingtonpost.com/g/page/national/nsa-signal-surveillance-success-stories/647/>). *The Washington Post*. Retrieved 28 January 2014.
252. ^a "Reporter: For NSA, Google cookies allow 'laser-guided' targeting" (http://www.washingtonpost.com/posttv/national/reporter-for-nsa-google-cookies-allow-laser-guided-targeting/2013/12/11/cd93fa24-62a1-11e3-aa81-e1dab1360323_video.html). *The Washington Post*. 11 December 2013. Retrieved 28 January 2014.
253. ^a Arne Halvorsen, Anne Marte Blindheim, Harald S. Klungtveit, Kjetil Magne Sørenes, Tore Bergsaker and Gunnar Hultgreen. "Norway's secret surveillance of Russian politics for the NSA" (<http://www.dagbladet.no/2013/12/17/nyheter/samfunn/politikk/utenriks/overvaking/30877258/>). *Dagbladet*. Retrieved 18 December 2013.

254. ^{a b c d e f} "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.
255. ^a Glenn Greenwald, Ryan Gallagher, Filip Struwe and Anna H Svensson. "SVT avslöjar: FRA spionerar på Ryssland åt USA" (<http://www.svt.se/nyheter/sverige/fra-spionerar-pa-ryssland-at-usa>) (in Swedish). Sveriges Television. Retrieved 5 December 2013.
256. ^a 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.
257. ^a Sven Bergman, Joachim Dyfvermark, Ryan Gallagher, Glenn Greenwald and Fredrik Laurin. "FRA spying on "energy" and "Baltics" for USA" (<http://www.svt.se/ug/fra-spying-on-energy-and-baltics-for-usa>). Sveriges Television. Retrieved 7 December 2013.
258. ^a "Cold War treaty confirms Sweden was not neutral" (<http://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-never-neutral>). *The Local*. Retrieved 12 December 2013.
259. ^a "NSA "asking for" specific exchanges from FRA - Secret treaty since 1954" (<http://www.svt.se/ug/nsa4>). Sveriges Television. Retrieved 12 December 2013.
260. ^a "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.
261. ^a Ashkan Soltani, Andrea Peterson, and Barton Gellman. "NSA uses Google cookies to pinpoint targets for hacking" (<http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/>). *The Washington Post*. Retrieved 12 December 2013.
262. ^a Greg Weston, Glenn Greenwald, Ryan Gallagher. "New Snowden docs show U.S. spied during G20 in Toronto" (<http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448>). Canadian Broadcasting Corporation. Retrieved 13 December 2013.
263. ^{a b c} Glenn Greenwald and Stefania Maurizi. "Revealed: How the NSA Targets Italy" (<http://espresso.repubblica.it/inchieste/2013/12/05/news/revealed-how-the-nsa-targets-italy-1.144428>). *L'espresso*. Retrieved 13 December 2013.
264. ^a MARK MAZZETTI and JUSTIN ELLIOTT (9 December 2013). "Spies Infiltrate a Fantasy Realm of Online Games" (<http://www.nytimes.com/2013/12/10/world/spies-drag-net-reaches-a-playing-field-of-elves-and-trolls.html>). *The New York Times*. Retrieved 12 December 2013.
265. ^a Ball, James (9 December 2013). "Xbox Live among game services targeted by US and UK spy agencies" (<http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life>). *The Guardian*. Retrieved 18 December 2013.
266. ^a "NSA files: games and virtual environments paper" (<http://www.theguardian.com/world/interactive/2013/dec/09/nsa-files-games-virtual-environments-paper-pdf>). *The Guardian*. 9 December 2013. Retrieved 18 December 2013.
267. ^a Justin Elliott, ProPublica, and Mark Mazzetti, The New York Times (9 December 2013). "NSA files: games and virtual environments paper" (<http://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games>). *Pro Publica*. Retrieved 18 December 2013.
268. ^a Craig Timberg and Ashkan Soltani. "By cracking cellphone code, NSA has capacity for decoding private conversations" (http://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.
269. ^a "How the NSA pinpoints a mobile device" (<http://apps.washingtonpost.com/g/page/world/how-the-nsa-pinpoints-a-mobile-device/645/#document/p2/a135576>). *The Washington Post*. Retrieved 14 December 2013.
270. ^a Leon, Richard (16 December 2013). "Federal judge rules NSA program is likely unconstitutional a.k.a. Klayman et al. v. Obama et al. Memorandum and Opinion from December 16, 2013 in Civil Action 13-0851 in United Case District Court for the District of Columbia" (<http://apps.washingtonpost.com/g/page/world/federal-judge-rules-nsa-program-is-likely-unconstitutional/668/>). *The Washington Post*. Retrieved 17 December 2013.
271. ^a Savage, Charlie (16 December 2013). "Judge Questions Legality of N.S.A. Phone Records" (<http://www.nytimes.com/2013/12/17/us/politics/federal-judge-rules-against-nsa-phone-data-program.html>). *The New York Times*. Retrieved 18 December 2013.
272. ^a Bill Mears and Evan Perez, CNN (17 December 2013). "Judge: NSA domestic phone data-mining unconstitutional" (<http://edition.cnn.com/2013/12/16/justice/nsa-surveillance-court-ruling/>). *cnn*. Retrieved 18 December 2013.

273. [^] Kravets, David (16 December 2013). "Court Says NSA Bulk Telephone Spying Is Unconstitutional" (<http://www.wired.com/threatlevel/2013/12/bulk-telephone-metada-ruling/>). Retrieved 18 December 2013.
274. [^] Kevin Johnson and Richard Wolf (16 December 2013). "Federal judge rules against NSA spying" (<http://www.usatoday.com/story/news/nation/2013/12/16/judge-nsa-surveillance-fourth-amendment/4041995/>). *USA Today*. Retrieved 18 December 2013.
275. [^] Gerstein, Josh (16 December 2013). "Judge: NSA phone program likely unconstitutional" (<http://www.politico.com/story/2013/12/national-security-agency-phones-judge-101203.html>). *Politico*. Retrieved 18 December 2013.
276. [^] ^a ^b Ellen Nakashima and Ann E. Marimow (16 December 2013). "Judge: NSA's collecting of phone records is probably unconstitutional" (http://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html). *The Washington Post*. Retrieved 17 December 2013.
277. [^] Spencer Ackerman and Dan Roberts (16 December 2013). "NSA phone surveillance program likely unconstitutional, federal judge rules" (<http://www.theguardian.com/world/2013/dec/16/nsa-phone-surveillance-likely-unconstitutional-judge>). *The Guardian*. Retrieved 18 December 2013.
278. [^] Pauley III, William H. (27 December 2013). "United States District Court Southern District of New York: American Civil Liberties Union v. James R. Clapper (13 Civ. 3994) (WHP))" (https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf). American Civil Liberties Union. Retrieved 28 December 2013.
279. [^] Adam Liptak and Michael S. Schmidt (27 December 2013). "Judge Upholds N.S.A.'s Bulk Collection of Data on Calls" (<http://www.nytimes.com/2013/12/28/us/nsa-phone-surveillance-is-lawful-federal-judge-rules.html?ref=us&pagewanted=all>). *The New York Times*. Retrieved 28 December 2013.
280. [^] Denniston, Lyle (27 December 2013). "Judge upholds NSA's phone data sweeps (UPDATED)" (<http://www.scotusblog.com/2013/12/judge-upholds-nsas-phone-data-sweeps/>). Scotusblog. Retrieved 28 December 2013.
281. [^] Peterson, Andrea (27 December 2013). "The most Kafkaesque paragraph from today's NSA ruling" (http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/27/the-most-kafkaesque-paragraph-from-todays-nsa-ruling/?wprss=rss_business). *The Washington Post*. Retrieved 28 December 2013.
282. [^] Horwitz, Sari (27 December 2013). "NSA collection of phone data is lawful, federal judge rules" (http://www.washingtonpost.com/world/national-security/nsa-collection-of-phone-data-is-lawful-federal-judge-rules/2013/12/27/4b99d96a-6f19-11e3-a523-fe73f0ff6b8d_story.html?hpid=z3). *The Washington Post*. Retrieved 28 December 2013.
283. [^] Ackermann, Spencer (2 January 2014). "ACLU will appeal ruling that NSA bulk phone record collection is legal" (<http://www.theguardian.com/world/2014/jan/02/aclu-appeal-nsa-bulk-phone-record-collection>). *The Guardian*. Retrieved 4 January 2014.
284. [^] James Glanz and Andrew W. Lehren (20 December 2013). "N.S.A. Spied on Allies, Aid Groups and Businesses" (<http://www.nytimes.com/2013/12/21/world/nsa-drag-net-included-allies-aid-groups-and-business-elite.html?src=recg&pagewanted=all>). *The New York Times*. Retrieved 28 December 2013.
285. [^] ^a ^b Jacob Appelbaum, Judith Horchert and Christian Stöcker. "Catalog Reveals NSA Has Back Doors for Numerous Devices - Shopping for Spy Gear: Catalog Advertises NSA Toolbox" (<http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>). *Der Spiegel*. Retrieved 30 December 2013.
286. [^] Jacob Appelbaum, Laura Poitras, Marcel Rosenbach, Christian Stöcker, Jörg Schindler and Holger Start. "Inside TAO: Documents Reveal Top NSA Hacking Unit - The NSA Uses Powerful Toolbox in Effort to Spy on Global Networks" (<http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html>). *Der Spiegel*. Retrieved 30 December 2013.
287. [^] "Interactive Graphic: The NSA's Spy Catalog" (<http://www.spiegel.de/international/world/a-941262.html>). *Der Spiegel*. 30 December 2013. Retrieved 4 January 2014.
288. [^] Erik Kain (2013-12-29). "Report: NSA Intercepting Laptops Ordered Online, Installing Spyware" (<http://www.forbes.com/sites/erikkain/2013/12/29/report-nsa-intercepting-laptops-ordered-online-installing-spyware/>). Retrieved 30 December 2013.
289. [^] RAPHAEL SATTER (29 December 2013). "Report: NSA intercepts computer deliveries" (http://hosted.ap.org/dynamic/stories/E/EU_NSA_SURVEILLANCE?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2013-12-29-13-01-13). Associated Press. Retrieved 30 December 2013.

290. ^ Courtney Subramanian (Dec 29, 2013). "The TAO of the NSA: Specialized Hacking Team Gets the 'Ungettable'" (<http://world.time.com/2013/12/29/the-cao-of-the-nsa-specialized-hacking-team-gets-the-ungettable/>). *Time (magazine)*. Retrieved 30 December 2013.
291. ^ "Glenn Greenwald: The NSA Can "Literally Watch Every Keystroke You Make"" (http://www.democracynow.org/2013/12/30/glenn_greenwald_the_nsa_can_literally). *Democracy Now!*. Democracy Now!. 30 December 2013. Retrieved 4 January 2014.
292. ^ Walters, Joanna (29 December 2013). "NSA 'hacking unit' infiltrates computers around the world – report" (<http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-cao>). *The Guardian*. Retrieved 4 January 2014.
293. ^ "GHOSTMACHINE: The NSA's cloud analytics platform" (<http://apps.washingtonpost.com/g/page/world/ghostmachine-the-nas-cloud-analytics-platform/644/>). *The Washington Post*. Retrieved 28 December 2013.
294. ^ http://www.theregister.co.uk/2013/12/10/french_gov_dodgy_ssl_cert_reprimand/
295. ^ ^a ^b Michael Winter (January 2, 2014). "NSA working to build computer to crack encryption" (<http://www.usatoday.com/story/news/nation/2014/01/02/nsa-computer-break-encryption/4294871/>). *USA Today*. Retrieved 3 January 2014.
296. ^ ^a ^b ^c Steven Rich and Barton Gellman (3 January 2014). "NSA seeks to build quantum computer that could crack most types of encryption" (http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html). *The Washington Post*. Retrieved 3 January 2014.
297. ^ "A description of the Penetrating Hard Targets project" (<http://apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/>). *The Washington Post*. 2 January 2014. Retrieved 4 January 2014.
298. ^ "Classifying NSA quantum computing efforts" (<http://apps.washingtonpost.com/g/page/world/classifying-nsa-quantum-computing-efforts/692/>). *The Washington Post*. 2 January 2014. Retrieved 4 January 2014.
299. ^ Lee, Timothy B. (2 January 2014). "Confused about the NSA's quantum computing project? This MIT computer scientist can explain." (<http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/02/confused-about-the-nas-quantum-computing-project-this-mit-computer-scientist-can-explain/>). *The Washington Post*. Retrieved 4 January 2014.
300. ^ "Report: NSA 'collected 200m texts per day'" (<http://www.bbc.co.uk/news/world-us-canada-25770313>). BBC. Retrieved 16 January 2014.
301. ^ Geoff White (16 January 2014). "Revealed: UK and US spied on text messages of Brits" (<http://www.channel4.com/news/intercept-text-messages-spy-nsa-gchq-british-phone>). Channel 4. Retrieved 16 January 2014.
302. ^ ^a ^b ^c ^d ^e ^f James Ball in (16 January 2014). "NSA collects millions of text messages daily in 'untargeted' global sweep" (<http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>). *The Guardian*. Retrieved 16 January 2014.
303. ^ "Report: NSA 'collected 200m texts per day'" (<http://www.bbc.co.uk/news/world-us-canada-25770313>). BBC. Retrieved 16 January 2014.
304. ^ James Glanz, Jeff Larson and Andrew W. Lehren (27 January 2014). "Spy Agencies Tap Data Streaming From Phone Apps - A version of the NYT appeared in print on January 28, 2014, on page A1 of the New York edition with the headline: Spy Agencies Tap Data Streaming From Phone Apps." (http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?hp&_r=1). *The New York Times*. Retrieved 28 January 2014.
305. ^ "From Britain's Government Communications Headquarters" (<http://www.nytimes.com/interactive/2014/01/28/world/28mobile-annotateB.html>). *The New York Times*. 27 January 2014. Retrieved 28 January 2014.
306. ^ ^a ^b "From the National Security Agency" (http://www.nytimes.com/interactive/2014/01/28/world/28mobile-annotateA.html?_r=0). *The New York Times*. 27 January 2014. Retrieved 28 January 2014.
307. ^ Ball, James (28 January 2014). "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data" (<http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>). *Th Guardian*. Retrieved 28 January 2014.
308. ^ Jeff Larson, ProPublica, and James Glanz and Andrew W. Lehren, The New York Times (27 January 2014). "Spy Agencies Probe Angry Birds and Other Apps for Personal Data" (<http://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data>). *ProPublica*. Retrieved 28 January 2014.
309. ^ Ball, James (27 January 2014). "NSA and GCHQ target 'leaky' phone apps like Angry Birds to scoop user data" (<http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>). *The Guardian*. Retrieved 27 January 2014.

310. ^ JAMES GLANZ, JEFF LARSON and ANDREW W. LEHREN (27 January 2014). "Spy Agencies Scour Phone Apps for Personal Data" (<http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html>). *The New York Times*. Retrieved 27 January 2014.
311. ^ Richard Esposito, Matthew Cole, Mark Schone, Glenn Greenwald (27 January 2014). "Snowden docs reveal British spies snooped on YouTube and Facebook" (http://investigations.nbcnews.com/_news/2014/01/27/22469304-snowden-docs-reveal-british-spies-snooped-on-youtube-and-facebook?lite). NBC News. Retrieved 27 January 2014.
312. ^ "Psychology A New Kind of SIGDEV (Signals Development) - Establishing the Human Science Operation Cell" (http://msnbcmedia.msn.com/i/msnbc/Sections/NEWS/snowden_youtube_nbc_document.pdf). *GCHQ*. NBC News Investigations. 27 January 2014. Retrieved 28 January 2014.
313. ^ Foreign press: Angry Birds apps may be used for spying (http://yle.fi/uutiset/foreign_press_angry_birds_apps_may_be_used_for_spying/7057219) yle 28.1.2014 19
314. ^ Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data (<http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>) the Guardian 27.1.2014 19
315. ^ Mike Dorning and Chris Strohm (Aug 23, 2013). "Court Finding of Domestic Spying Risks Obama Credibility" (<http://www.bloomberg.com/news/2013-08-23/court-finding-of-domestic-spying-risks-obama-credibility.html>). Bloomberg Television. Retrieved 28 December 2013.
316. ^ Adam Serwer (08/07/13). "Obama says 'there is no spying on Americans,' but what about our data?" (<http://www.msnbc.com/msnbc/obama-says-there-no-spying-americans>). MSNBC. Retrieved 28 December 2013.
317. ^ "Press Briefing by Press Secretary Jay Carney, 6/13/2013" (<http://www.whitehouse.gov/the-press-office/2013/06/13/press-briefing-press-secretary-jay-carney-6132013>). White House. Retrieved 28 December 2013.
318. ^ "Holder: Leaks damaged U.S. security" (<http://edition.cnn.com/2013/06/14/world/europe/nsa-leaks/>). CNN. June 15, 2013. Retrieved 28 December 2013.
319. ^ "Cameron says may act against press over spy leaks" (<http://uk.reuters.com/article/2013/10/28/uk-usa-spying-cameron-idUKBRE99O0K120131028>). Reuters. Oct 28, 2013. Retrieved 28 December 2013.
320. ^ Janet Stobart (June 10, 2013). "Britain denies using PRISM to get around domestic spying laws" (<http://articles.latimes.com/2013/jun/10/world/la-fg-wn-britain-nsa-prism-surveillance-program-20130610>). *The Los Angeles Times*. Retrieved 28 December 2013.
321. ^ Rob Williams (10 October 2013). "Snowden leaks published by the Guardian were damaging to security, says Nick Clegg" (<http://www.independent.co.uk/news/uk/politics/snowden-leaks-published-by-the-guardian-were-damaging-to-security-says-nick-clegg-8871894.html>). *The Independent*. Retrieved 1 January 2014.
322. ^ "Abbott offers Australian spy assurance" (<http://www.theaustralian.com.au/national-affairs/abbott-offers-australian-spy-assurance/story-fn59niix-1226750534569>). *The Australian*. October 31, 2013. Retrieved 30 December 2013.
323. ^ "Germany's Merkel rejects NSA-Stasi comparison" (<http://bigstory.ap.org/article/germanys-merkel-rejects-nsa-stasi-comparison>). Associated Press. Jul 10, 2013. Retrieved 28 December 2013.
324. ^ "German Interior Minister Friedrich Discusses NSA Spying Affair" (<http://www.spiegel.de/international/germany/german-interior-minister-friedrich-discusses-nsa-spying-affair-a-918770.html>). Der Spiegel. August 28, 2013. Retrieved 28 December 2013.
325. ^ "Carl Bildt defends FRA surveillance as 'necessary'" (<http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5733081>). Sveriges Radio. Retrieved 28 December 2013.
326. ^ "Germany probes secret service ties with US agencies" (<http://www.google.com/hostednews/afp/article/ALeqM5i8cOrcBcm1S4CxaYoU8CP75GJpw?docId=CNG.13941495f3f18c4f09f35348610dab3f.921>). Agence France-Presse. Retrieved 28 December 2013.
327. ^ William Boston (July 22, 2013). "Germany to Review Spy Service's Ties With NSA" (<http://online.wsj.com/news/articles/SB10001424127887324783204578621920253442796>). The Wall Street Journal. Retrieved 28 December 2013.
328. ^ Mike Levine. "White House Picks Panel to Review NSA Programs" (<http://abcnews.go.com/blogs/politics/2013/08/white-house-picks-panel-to-review-nsa-programs/>). ABC News. Retrieved 28 December 2013.
329. ^ Johnson, Luke. "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 August 13, 2013.

330. [^] Nick Hopkins, Patrick Wintour, Rowena Mason and Matthew Taylor (17 October 2013). "Extent of spy agencies' surveillance to be investigated by parliamentary body" (<http://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden>). *The Guardian*. Retrieved 28 December 2013.
331. [^] Stewart Bell (December 9, 2013). "Review underway into allegations that national intelligence agency illegally spied on Canadians" (<http://news.nationalpost.com/2013/12/09/review-underway-into-allegations-that-national-intelligence-agency-illegally-spied-on-canadians/>). *National Post*. Retrieved 30 December 2013.
332. [^] Edward Lucas (23 January 2014), The Snowden Operation: Inside the West's Greatest Intelligence Disaster (<http://www.amazon.com/The-Snowden-Operation-Greatest-Intelligence-ebook/dp/B00I0W61OY>) ASIN:B00I0W61OY
333. [^] Bob Cesca (27 January 2014), NSA Agent's Identity Exposed in Poorly-Redacted Snowden Document (<http://thedailybanter.com/2014/01/the-name-of-an-nsa-agent-exposed-in-poorly-redacted-snowden-document/>) *The Daily Banter*]]
334. [^] Andrei Soldatov (8 January 2014), ИТОГИ ГОДА. СПЕЦСЛУЖБЫ (<http://www.ej.ru/?a=note&id=24044>) *ежедневный журнал*
335. [^] Montevideo Statement on the Future of Internet Cooperation (<http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm>) ICANN 7 October 2013
336. [^] ^a ^b ^c Ewen MacAskill and Dominic Rushe. "Snowden document reveals key role of companies in NSA data collection" (<http://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms>). *The Guardian*. Retrieved 22 December 2013.
337. [^] "Collateral Murder, 5 Apr 2010" (http://wikileaks.org/wiki/Collateral_Murder,_5_Apr_2010). WikiLeaks. April 5, 2010. Retrieved 1 January 2014.
338. [^] "Afghan War diary" (<http://wikileaks.org/afg/>). WikiLeaks. July 25, 2010. Retrieved 1 January 2014.
339. [^] "Iraq War logs" (<http://wikileaks.org/irq/>). WikiLeaks. October 22, 2010. Retrieved 1 January 2014.
340. [^] "Secret US Embassy Cables" (<http://wikileaks.org/cablegate.html>). WikiLeaks. November 28, 2010. Retrieved 1 January 2014.
341. [^] "Gitmo Files" (<http://wikileaks.org/gitmo/>). WikiLeaks. April 24, 2011. Retrieved 1 January 2014.

External links

 Media related to 2013 Mass Surveillance Disclosures at Wikimedia Commons

- "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" (<http://www.guardian.co.uk/world/the-nsa-files>). *The Guardian*.
- *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*. June 13, 2013.
- NSA inspector general report on email and internet data collection under Stellar Wind (<http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection>) as provided by The Guardian on June 27, 2013.
- "Putin talks NSA, Syria, Iran, drones in exclusive RT interview (FULL VIDEO) (<https://www.youtube.com/watch?v=33oIF-ggK5U>)." *Russia Today*. June 12, 2013.
- Ackerman, Spencer. "NSA warned to rein in surveillance as agency reveals even greater scope (<http://www.guardian.co.uk/world/2013/jul/17/nsa-surveillance-house-hearing>)." *The Guardian*. July 17, 2013.
- Ackerman, Spencer. "Slew of court challenges threaten NSA's relationship with tech firms (<http://www.guardian.co.uk/world/2013/jul/17/nsa-court-challenges-tech-firms>)." *The Guardian*. Wednesday July 17, 2013.
- Ackerman, Spencer and Paul Lewis. "NSA amendment's narrow defeat spurs privacy advocates for surveillance fight (<http://www.guardian.co.uk/world/2013/jul/25/narrow-defeat-nsa-amendment-privacy-advocates>)." *The Guardian*. Thursday July 25, 2013.

- Ackerman, Spencer and Dan Roberts. "US embassy closures used to bolster case for NSA surveillance programs (<http://www.theguardian.com/world/2013/aug/05/us-embassy-closure-nsa-surveillance>).\" *The Guardian*. Monday August 5, 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 (<http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access>).\" *The Guardian*. Sunday August 4, 2013.
- "Obama's former adviser ridicules statement that NSA doesn't spy on Americans (<http://rt.com/usa/us-obama-surveillance-snowden-296/>).\" (Archive (<http://archive.is/sLrba>)) *Russia Today*. August 9, 2013.
- MacAskill, Ewen. "Justice Department fails in bid to delay landmark case on NSA collection (<http://www.guardian.co.uk/world/2013/jul/25/justice-department-case-nsa-collection>).\" *The Guardian*. Thursday July 25, 2013.
- Rushe, Dominic. "Microsoft pushes Eric Holder to lift block on public information sharing (<http://www.guardian.co.uk/technology/2013/jul/16/microsoft-eric-holder-permission-information-national-security>).\" *The Guardian*. Tuesday July 16, 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 (<http://archive.is/MqsdK>)) *CNN*. August 9, 2013.
- Gellman, Barton. "NSA broke privacy rules thousands of times per year, audit finds (http://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 August 15, 2013.
- Roberts, Dan and Robert Booth. "NSA defenders: embassy closures followed pre-9/11 levels of 'chatter' (<http://www.theguardian.com/world/2013/aug/04/nsa-us-embassy-closures-terrorist-threat>).\" *The Guardian*. Sunday August 4, 2013.
- Greenwald, Glenn. "The crux of the NSA story in one phrase: 'collect it all' (<http://www.guardian.co.uk/commentisfree/2013/jul/15/crux-nsa-collect-it-all>).\" *The Guardian*. Monday July 15, 2013.
- Sanchez, Julian. "Five things Snowden leaks revealed about NSA's original warrantless wiretaps (<http://arstechnica.com/tech-policy/2013/07/5-things-snowden-leaks-revealed-about-nas-original-warrantless-wiretaps/>).\" *Ars Technica*. July 9, 2013.
- Forero, Juan. "Paper reveals NSA ops in Latin America (http://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*. July 9, 2013.
- Jabour, Bridie. "Telstra signed deal that would have allowed US spying (<http://www.guardian.co.uk/world/2013/jul/12/telstra-deal-america-government-spying>).\" *The Guardian*. Friday July 12, 2013.
- Ackerman, Spencer. "White House stays silent on renewal of NSA data collection order (<http://www.guardian.co.uk/world/2013/jul/18/white-house-silent-renewal-nsa-court-order#start-of-comments>).\" *The Guardian*. Thursday July 18, 2013.
- Naughton, John. "Edward Snowden's not the story. The fate of the internet is (<http://www.guardian.co.uk/technology/2013/jul/28/edward-snowden-death-of-internet>).\" *The Guardian*. July 28, 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*. August 8, 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*. June 10, 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 (<http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations>)" by the Guardian's James Ball on August 21, 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" (<http://wikileaks.org/the-spyfiles.html>). *Wikileaks*. December 1, 2011. A collection of documents relating to surveillance.
 - "The Spy Files" (<http://wikileaks.org/spyfiles/list/releasedate/2011-12-08.html>). *Wikileaks*. December 8, 2011. Part 2 of the above.
 - "Spy Files 3" (<http://wikileaks.org/spyfiles3.html>). *Wikileaks*. September 4, 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-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html>) (in Portuguese). September 2, 2013. Retrieved September 4, 2013. Documents relating to the surveillance against Dilma Roussef 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 (<http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>) by The Guardian's Bruce Schneier on September 5, 2013.
- 2014-01-04 Al Jazeera's "Listening Post - The Snowden saga: Spies, secrets and security - A look back at the biggest media story of 2013 - Edward Snowden and the NSA surveillance programme." (<http://www.youtube.com/watch?v=9IjtsED5Iy8&sns=em>) The first part of the broadcast retells the global surveillance in the year 2013 and the second part shows an interview former NSA general counsel Stewart Baker.

Retrieved from "[http://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosures_\(2013–present\)&oldid=593019838](http://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosures_(2013–present)&oldid=593019838)"

Categories: Global surveillance

-
- This page was last modified on 29 January 2014 at 21:43.
 - 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.

From Wikipedia, the free encyclopedia

Article policies

- No original research
- Neutral point of view
- Verifiability



Mid

This article has been rated as **Mid-importance** on the project's importance scale.

WikiProject United States / Government (Rated B-class, Mid-importance)



This article is within the scope of **WikiProject United States**, a collaborative effort to improve the coverage of topics relating to the United States of America on Wikipedia. If you would like to participate, please visit the project page, where you can join the ongoing discussions.

Template Usage • **Articles Requested!** • Become a Member • Project Talk • Unreferenced BLPs • Alerts

B

This article has been rated as **B-Class** on the project's quality scale.

Mid

This article has been rated as **Mid-importance** on the project's importance scale.







This article is supported by **WikiProject U.S. Government**.

WikiProject U.S. Government To-do:

edit ([//en.wikipedia.org/w/index.php?title=Wikipedia:WikiProject_United_States_Government/to_do&action=edit](http://en.wikipedia.org/w/index.php?title=Wikipedia:WikiProject_United_States_Government/to_do&action=edit)) • history ([//en.wikipedia.org/w/index.php?title=Wikipedia:WikiProject_United_States_Government/to_do&action=history](http://en.wikipedia.org/w/index.php?title=Wikipedia:WikiProject_United_States_Government/to_do&action=history)) • watch ([//en.wikipedia.org/w/index.php?title=Wikipedia:WikiProject_United_States_Government/to_do&action=watch](http://en.wikipedia.org/w/index.php?title=Wikipedia:WikiProject_United_States_Government/to_do&action=watch)) • purge ([//en.wikipedia.org/w/index.php?title=Talk:Global_surveillance_disclosures_\(2013%E2%80%93present\)&action=purge](http://en.wikipedia.org/w/index.php?title=Talk:Global_surveillance_disclosures_(2013%E2%80%93present)&action=purge))

Funk

Here are some **tasks you can do**:

- **Article requests:** Bring Federal government of the United States to GA. Rescue *99 Percent Declaration* from deletion.
- **Cleanup:** United States Government articles needing attention, Federal government of the United States#Executive branch
- **Expand:** Office of Surface Mining, General Land Office
- **Featured article candidates:** No results were found.
- **Featured list candidates:** No results were found.
- **Featured sound candidates:** No results were found.
- **Good article nominations:**
 -  Idaho v. United States
 -  United States Senate election in Massachusetts, 2012
 -  Voting Rights Act of 1965
 -  Alexander White (Virginia)
- **Infobox:** United States Government articles needing infoboxes
- **Map:** Wikipedia requested maps of the United States Government
- **Photo:** Requested photographs of the United States Government
- **Stubs:** Stub-Class United States Government articles, Category:United States government stubs, Bureau of Engraving and Printing
- **Update:** U.S. Food and Drug Administration, United States House of Representatives elections in California, 2008; United States House of Representatives elections in Idaho, 2006, United States House of Representatives elections in Nevada, 2006; United States mayoral elections, 2007

- **Unreferenced:** Unreferenced United States Government articles
- **Verify:** Bureau of Reclamation, United States Grazing Service, General Land Office, Bureau of Land Management, Bureau of Engraving and Printing, Factions in the Republican Party
- **Other:**
 - List of U.S. states by GDP per capita (nominal) is self contradictory
 - Place the {{WikiProject United States|class=|importance=|USGov=Yes|USGov-importance=}} banner into United States Government related articles and assess

WikiProject Politics of the United Kingdom

(Rated B-class, Mid-importance)



This article is within the scope of **WikiProject Politics of the United Kingdom**, a collaborative effort to improve the coverage of Politics of the United Kingdom on Wikipedia. If you would like to participate, please visit the project page, where you can join the discussion and see a list of open tasks.

B

This article has been rated as **B-Class** on the project's quality scale.

This article has been checked against the following **criteria** for B-Class status:



1. ✓ Referencing and citation: *criterion met*
2. ✓ Coverage and accuracy: *criterion met*
3. ✓ Structure: *criterion met*
4. ✓ Grammar and style: *criterion met*
5. ✓ Supporting materials: *criterion met*
6. ✓ Accessibility: *criterion met*

Mid

This article has been rated as **Mid-importance** on the project's importance scale.



Text from this version ([//en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&oldid=583596559](http://en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&oldid=583596559)) of 2013 global surveillance disclosures was copied or moved into Global surveillance disclosure with this edit ([//en.wikipedia.org/w/index.php?title=Global_surveillance_disclosure&diff=prev&oldid=583602404](http://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosure&diff=prev&oldid=583602404)) on 00:48, 28 November 2013. The former page's history ([//en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&action=history](http://en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&action=history)) now serves to provide attribution for that content in the latter page, and it must not be deleted so long as the latter page exists. The former page's talk page can be accessed at [Talk:2013 global surveillance disclosures](http://Talk:2013_global_surveillance_disclosures).



Text from this version ([//en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&oldid=583855862](http://en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&oldid=583855862)) of 2013 global surveillance disclosures was copied or moved into Global surveillance disclosure with this edit ([//en.wikipedia.org/w/index.php?title=Global_surveillance_disclosure&diff=prev&oldid=588625542](http://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosure&diff=prev&oldid=588625542)) on 2014-01-01T06:09:59. The former page's history ([//en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&action=history](http://en.wikipedia.org/w/index.php?title=2013_global_surveillance_disclosures&action=history)) now serves to provide attribution for that content in the latter page, and it must not be deleted so long as the latter page exists. The former page's talk page can be accessed at [Talk:2013 global surveillance disclosures](http://Talk:2013_global_surveillance_disclosures).

Contents

- 1 Orphaned references in Timeline of mass surveillance disclosures
- 2 NSA primary sources
- 3 Findings on Italy
- 4 NSA and AT&T and how NSA collects data
- 5 Scope of article
- 6 More sources
- 7 (N)POV re: foreign nationals / US citizens
- 8 Bill Clinton on spying
- 9 Merkel-Obama meeting
- 10 EU parliament meeting
- 11 Proposal: rename to "2013 Global surveillance disclosures"
- 12 New sources
- 13 How GCHQ Monitors Germany, Israel and the EU
- 14 NSA Reportedly Paid A Security Firm Millions To Ship Deliberately Flawed Encryption Technology
- 15 N.S.A. Spied on Allies, Aid Groups and Businesses
- 16 2013 in Review: The Year the NSA Finally Admitted Its "Collect It All" Strategy
- 17 Additional new sources
- 18 NSA capabilities with its TAO
- 19 DROPOUTJEEP
- 20 ACLU sues US government
- 21 Proposal to remove references not publicly available.
- 22 Section clarification.
- 23 How the NSA Threatens National Security
- 24 Former NSA whistleblowers plead for chance to brief Obama on agency abuses
- 25 N.S.A. Devises Radio Pathway Into Computers
- 26 NSA collects millions of text messages daily in 'untargeted' global sweep
- 27 Broken Redirect
- 28 Orphaned references in Global surveillance disclosures (2013–present)
- 29 Invitation to help craft a proposal
- 30 Reactions of political leaders

Orphaned references in Timeline of mass surveillance disclosures

I check pages listed in Category:Pages with incorrect ref formatting to try to fix reference errors. One of the things I do is look for content for orphaned references in wikilinked articles. I have found content for some of Timeline of mass surveillance disclosures's orphans, the problem is that I found more than one version. I can't determine which (if any) is correct for *this* article, so I am asking for a sentient editor to look it over and copy the correct ref content into this article.

Reference named "http":

- From Cyberwarfare: *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*, Vol. 8, Iss. 1 [October 2008], Art. 2. pp.42 (2008). <http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm> (2008). (<http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm>) |url= missing title (help). Retrieved January 2013.
- From 2013 global surveillance disclosures: Barton Gellman and Matt DeLong (August 15, 2013). "First direct evidence of illegal surveillance found by the FISA court" (<http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393/>). *The Washington Post*. Retrieved September 16, 2013.

Reference named "WP20130830":

- From Blarney (code name): Craig Timberg and Barton Gellman (30 August 2013). "NSA paying U.S. companies for access to communications networks" (http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html). *The Washington Post*. Retrieved 31 August 2013.
- From 2013 global surveillance disclosures: Craig Timberg and Barton Gellman (August 30, 2013). "NSA paying U.S. companies for access to communications networks" (http://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html). *The Washington Post*. Retrieved August 31, 2013.

I apologize if any of the above are effectively identical; I am just a simple computer program, so I can't determine whether minor differences are significant or not. AnomieBOT✉ 01:31, 28 November 2013 (UTC)

NSA primary sources

This (<https://www.eff.org/nsa-spying/nsadocs>) looks to be a fantastic resource - it's a rundown of the leaks thus far, with links to their respective RS. petrarchan47tc 04:02, 28 November 2013 (UTC)

Findings on Italy

English article:

- Greenwald, Glenn and Stefania Maurizi. "Revealed: How the Nsa Targets Italy (<http://espresso.repubblica.it/inchieste/2013/12/05/news/revealed-how-the-nsa-targets-italy-1.144428/>)." *L'Espresso*. 5 December 2013.

WhisperToMe (talk) 02:38, 7 December 2013 (UTC)

NSA and AT&T and how NSA collects data

- Mendoza, Martha. "AT&T: We don't have to disclose NSA dealings (<http://www.usatoday.com/story/money/business/2013/12/06/att-says-it-doesnt-have-to-disclose-nsa-dealings/3894823/>)." *Associated Press* at the *USA Today*. December 6, 2013.
- "How the NSA is tracking people right now (<http://apps.washingtonpost.com/g/page/world/how-the-nsa-is-tracking-people-right-now/634/>)." *The Washington Post*.

WhisperToMe (talk) 21:01, 7 December 2013 (UTC)

Scope of article

Should this article be limited to the contents of disclosures only? Or should we include some background details about the spy agreements related to Snowden's documents? -A1candidate (talk) 14:39, 8 December 2013 (UTC)

If the content is limited to the current subject matter, I think that the title is wrong. There is no context as to what "Global surveillance disclosure" means. I appreciate that you are now asking for feedback. However, I think that there should have been more consultation on the 2013 mass surveillance disclosures page and consensus reached before these extensive changes were made. There was a discussion starting at Talk:2013 global surveillance disclosures#Size of article which is now hidden behind a redirect. Major changes such as these need to be spelled out and agreed to by consensus before they are carried out, IMO. The discussion had only just begun and there was no general agreement. I have concerns about these changes. I won't list them all just now, except to say that there is little context given in several of these articles to let the reader know clearly what they are about. It would have been far easier to start from the original "2013 mass surveillance disclosures" article and begin to establish sub articles. In support of your proposal, I suggested that we begin by establishing sub articles (and had set up one as an example of

what I meant). However, I stated that we should keep the original root article until we had created sub articles. One editor agreed with me and there were no other comments when you peremptorily made these massive changes. This is not collaborative editing. We need to figure out how to address this. Suggestions? Sunray (talk) 18:55, 8 December 2013 (UTC)

I continue to agree that the title and presentation needs to be discussed. It seems the titles of 3 Snowden-related pages (timeline, aftermath and this one) have now switched to the singular when referring to the disclosures, increasing the confusion and diversion from RS. Also, we need to get clear on whether the NSA is indeed leading this global surveillance (RS seems to indicate this), and whether the disclosures and surveillance we're talking about are directly related to Snowden, as RS indicates, and if so, make needed changes to these articles to make this clear. I see a pull towards "it's not the NSA, it's everyone" and a downplaying of the source of all of this: Edward Snowden. **petrarchan47**tc 23:15, 18 December 2013 (UTC)

More sources

- "Sweden helps the US spy on the Baltics: report (<https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5726836>)." *Radio Sweden*. 7 December 2013.
- "NSA tracks billions of intl cell phones daily – on Reagan's orders (<http://rt.com/usa/nsa-global-phone-tracking-875/>)." *Russia Today*. 7 December 2013. Updated 8 December 2013.
- "Sweden helped the NSA spy on Russia: report (<https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5724419>)." *Radio Sweden*. 5 December 2013.

WhisperToMe (talk) 02:48, 9 December 2013 (UTC)

- "Spy agencies in covert push to infiltrate virtual world of online gaming (<http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life>)." *The Guardian*. December 9, 2013.
 - NSA Document: <http://www.theguardian.com/world/interactive/2013/dec/09/nsa-files-games-virtual-environments-paper-pdf>

WhisperToMe (talk) 20:25, 9 December 2013 (UTC)

- Timberg, Craig and Ashkan Soltani. "By cracking cellphone code, NSA has capacity for decoding private conversations (http://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?hpid=z1)." *Washington Post*. December 13, 2013.
- Nakashima, Ellen. "White House to preserve controversial policy on NSA, Cyber Command leadership (http://www.washingtonpost.com/world/national-security/white-house-to-preserve-controversial-policy-on-nsa-cyber-command-leadership/2013/12/13/4bb56a48-6403-11e3-a373-0f9f2d1c2b61_story.html?p=1)." *Washington Post*. December 13, 2013.

WhisperToMe (talk) 05:59, 16 December 2013 (UTC)

(N)POV re: foreign nationals / US citizens

Just a quick suggestion: Should not the english language version of Wikipedia appeal equally to all english-speaking people(s)? Or is the general meaning that this is the U.S. version? In the article's leading section, there is the phrase: "foreign nationals as well as US citizens", implying that everyone not a US citizen is a foreigner. In my opinion this is not a neutral point of view, but a US-centric one. Please also see the map showing countries in which English is the main or secondary language in the article about the English_Wikipedia. I therefore suggest rephrasing that fragment. — Preceding unsigned comment added by Phellmon (talk • contribs) 01:23, 10 December 2013 (UTC)

Bill Clinton on spying

- "Bill Clinton says security does not justify espionage (<http://news.xinhuanet.com/english/world/2013-12>

/10/c_132954580.htm)." (Archive (<http://archive.is/sbA2K>)) *Xinhua*. December 10, 2013.

WhisperToMe (talk) 08:21, 11 December 2013 (UTC)

Merkel-Obama meeting

- Traynor, Ian. "Merkel compared NSA to Stasi in heated encounter with Obama (<http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama>)." *The Guardian*. December 17, 2013.

WhisperToMe (talk) 09:11, 18 December 2013 (UTC)

EU parliament meeting

- "NSA's goal is elimination of individual privacy worldwide - Greenwald to EU (<http://rt.com/news/greenwald-eu-parliament-testimony-424/>)." (Archive (<http://archive.is/9qpnF>)) *Russia Today*. December 18, 2013.
 - Video: http://img.rt.com/files/news/21/8d/00/00/1150443_grenwald_full_480p.mp4?event=download -

WhisperToMe (talk) 16:45, 18 December 2013 (UTC)

Proposal: rename to "2013 Global surveillance disclosures"

I think the scope of this article is too broad. The first half talks about the chronology of American global surveillance. However, they are not the subject of the article and should not be described at length. The focus should be on the disclosures. Also, listing everything in chronological order is too confusing. The article would be much better if we broke them down by technical aspects, legal authority/related court cases, popular reaction, economic effect, and perhaps diplomatic repercussions. Many of these subjects spill over into the scope of other articles, and should be linked accordingly, but please: lets keep the scope limited to the 2013 Snowden leaks. Thoughts? Rustyfence (talk) 07:08, 19 December 2013 (UTC)

The article is organised by the chronology of the disclosures, beginning in 1972. The pre-2013 section is mainly about the disclosures. Rustyfence has already moved this article from Global surveillance disclosure to 2013 Global surveillance disclosure, implicitly changing the scope of the article. The bulk of this article is about leaks by Edward Snowden; explicitly making it about them seems fine. Limiting it to 2013 might be a mistake, because more of Snowden's documents may be published after the end of this month. Something like "Edward Snowden disclosures" or the longer but less ambiguous "disclosures by Edward Snowden" ought to be good titles, if the article is to be only about the information released by him. He acknowledges having released the documents. —rybec 11:40, 19 December 2013 (UTC)

It might be useful to research how the Snowden leaks are referred to most often in RS. And since only 1% of the leaked material has been reported on thus far, it does seem a mistake to label them by the year rather than by the leaker. I wouldn't recommend "NSA leaks" either, as there have been multiple, albeit lesser-known, NSA leaks in the past. I would vote to call the article "Snowden NSA leaks". **petrarchan47**tc 06:09, 20 December 2013 (UTC)

Rybec's suggestions for the title are good too. And as Rustyfence says, if (since) the article is focused on the Snowden (not necessarily 2013) leaks, then background information should be presented in proper context, perhaps even splitting it off and leaving a small summary here. The Snowden leaks are an enormous story to cover and don't need the added weight of telling the history of American global surveillance. I also like Rusty's idea to cover each program, disclosure and fallout separately. I agree that chronological order is not a good way to present this material. **petrarchan47**tc 06:17, 20 December 2013 (UTC)

- I agree with Petrarchan47 that "Snowden NSA leaks" would be the best title for this article. My second choice would be "2013 Global surveillance disclosures." However, in either case, I think that it would be important to summarize the background of these disclosures—likely best done in a "History" section. Snowden's leaks were part of a process of disclosures that originated in the 1970s and related to patterns of mass surveillance that originated in World War II. All this needs to be covered, IMO, to give the reader adequate context. Sunray (talk) 19:49, 22 December 2013

(UTC)

Definitely - context is a must. However, the balance of text, as well as the title, should stick to the focus of the article. The context shouldn't need too much space, and "History of NSA leaks" should be a standalone article.
petrarchan47tc 03:21, 27 December 2013 (UTC)

I think a good compromise would be to create a new page for the history section and summarize the most important points within a single section here. -A1candidate (talk) 09:45, 28 December 2013 (UTC)

That would be good if we could tighten the scope of this article to Snowden's leaks, and refer to them as RS does. While it is true that a global surveillance web is being revealed by the leaks, we have to stick to using RS for our coverage. For the most part, the language and presentation used in this article diverges from RS, and leaves me confused. It's as if editors are trying to tell a story different from the one found in media. I suspect it's due to geo-location of editors, and the use of different media. In the US, RS refers to the Snowden leaks as NSA leaks, not mass or global surveillance leaks. It's hard to understand why we can't have an article that clearly covers Snowden leaks and fallout. By clearly, I mean refer to this information the same way most RS does. That was the original intent for this article. For such an important story, it's baffling that we are still discussing this problem.

petrarchan47tc 19:48, 28 December 2013 (UTC)

I've been looking at how RS refers to the subject of this article, and would love to hear what others are noticing as well. From the US media, this story is framed as "NSA", and very little attention is given to Five Eyes or to the willingness of 'most Western nations' to aid NSA surveillance. The introduction to this article does not sound like the coverage I am seeing. It doesn't mention "leaks" and "Snowden" in the same sentence, and there is no redirect here in case someone Googles "Snowden leaks" or "NSA leaks", as far as I am aware. The intro would be perfect for an overview article, but not one devoted to Snowden leaks. What do others think? How is this story told in your geo-location? Please bring links, and I will do the same. We should be able to figure out the scope and title as well as needed offshoot articles by looking at upcoming "end of the year" summaries, and their wording/presentation. **petrarchan47tc** 01:15, 31 December 2013 (UTC)

NSA leaks redirects to this article; I've just created Snowden leaks as a redirect to

Edward_Snowden#Leaks; NSA leaks is linked that section in the Snowden biography. —rybec 01:47, 31 December 2013 (UTC)

Brilliant! Now we need to review the Lede to this article, because it's really the Lede for a different (yet-to-be-created) article, an article that includes the full story of surveillance. Excuse my stating the obvious, but this article's Lede needs to make clear that the focus is on the Snowden leaks. **petrarchan47tc** 05:21, 1 January 2014 (UTC)

This discussion has stalled out. Does anyone object to changing the title to "2013 global surveillance disclosures"? If not I'll change it. --Dr. Fleischman (talk) 05:05, 4 January 2014 (UTC)

Well, we're in 2014 now, aren't we? -A1candidate (talk) 11:26, 4 January 2014 (UTC)

Sorry I'm late to this discussion. I do **object** to the proposed title change. These leaks are still occurring and there is speculation that other NSA employees or contractors are leaking documents. Also, all of the leaks should not be attributed to Snowden. For example, there is reason to believe that the NSA ANT catalog *may* have been leaked by someone other than Snowden. *Der Spiegel*/Applebaum have not implicated Snowden. I agree that the article has some scope ambiguity, and that there may be a better title (2012-2014 global surveillance disclosures?).- MrX 14:36, 4 January 2014 (UTC)

I too **object**. As MrX observes, the leaks are ongoing. In particular we should bear in mind that Snowden passed a huge cache to reporter Glenn Greenwald, who has been releasing them in a trickle. Moreover, Greenwald has announced a new journalistic venture, funded by billionaire Pierre Omidyar, and a book on this topic forthcoming in April. It's likely that Greenwald will use both his book and the Omidyar platform to publish additional disclosures from his repository of Snowden leaks. Changing the title so as to limit our article's scope to 2013, scarcely four days into 2014, is premature. JohnValeron (talk) 16:57, 4 January 2014 (UTC)

To reinforce my foregoing objection, on January 3, 2014, Glenn Greenwald appeared on Fox News, where he was asked: "You have a lot of additional information. Will you be releasing more? And if so,

when?"

"Oh, definitely," Greenwald replied. "You know, Edward Snowden said his job is done—meaning him as a whistleblower, he got the information to journalists—now our job as journalists is to inform the American people about what their government is doing to them. And there's a lot more stories coming in the early part of January—the first two or three months—that I think are going to be very, very interesting to Americans about what their government is doing to their privacy in the dark." JohnValeron (talk) 19:37, 4 January 2014 (UTC)

The story [1] (http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html) about NSA's efforts in quantum computing was first published in January 2014, and is mentioned in the article. —rybec 04:57, 5 January 2014 (UTC)

Any objection to "2013-2014 global surveillance disclosures"? --Dr. Fleischman (talk) 05:24, 5 January 2014 (UTC)

Yes, I **object** to your amended proposed name change as being premature and unnecessarily limiting to a subject that is still in the process of playing out. Cryptome reports that of the 1.7 million documents Snowden walked away with, only a few hundred have been made public, and estimates that at the present rate of release it'll take 42 years to publish the complete trove. See <http://cryptome.org/2013/11/snowden-tally.htm>. Why are you singularly intent on making this change only 2½ weeks after it was first proposed—what's the rush? JohnValeron (talk) 18:04, 5 January 2014 (UTC)

I only agree that the title should be plural. I'm not sure why it's necessary to include a date range though. WP:TITLE instructs us to create concise titles that are "no longer than necessary to identify the article's subject and distinguish it from other subjects." The fact is, we don't know that 2014 will be the end of these disclosures.- MrX 18:15, 5 January 2014 (UTC)

MrX, thanks for pointing that out. I focused on the dates and failed to notice adding "s" to disclosure. Yes, agreed, by all means it should be plural. But let's leave dates out of title. JohnValeron (talk) 19:16, 5 January 2014 (UTC)

Don't we have to distinguish the recent wave of disclosures from the ones that came before? (Some of those are covered at NSA warrantless surveillance (2001–07).) --Dr. Fleischman (talk) 22:56, 5 January 2014 (UTC)

The title "Global surveillance disclosures" distinguishes this article's subject matter from NSA warrantless surveillance (2001–07). Please note that the latter's lede begins: "The NSA warrantless surveillance controversy ('warrantless wiretapping') concerns surveillance of persons *within the United States* who were in contact with 'terrorists' during the collection of foreign intelligence by the U.S. National Security Agency (NSA) as part of the war on terror." (Emphasis added.) The first word in the successor article's title—**Global**—immediately differentiates it from domestic surveillance. JohnValeron (talk) 00:24, 6 January 2014 (UTC)

Maybe we should just pluralize the title now, and then consider adding a range of years after this spate of disclosures is clearly over.- MrX 16:36, 6 January 2014 (UTC)

I concur with MrX. In his blog today, Glenn Greenwald (the keeper of Snowden's unreleased leaks) writes that "there are many, many more that will be published in the short-term. ... Our work is very far from done: there are many, many more documents and stories that we will publish." See <http://utdocuments.blogspot.com.br/2014/01/email-exchange-with-reader-over-first.html> Given the enormous volume of the Snowden cache, I doubt Greenwald's piecemeal release will be complete by the end of 2014. For now, we should just pluralize our title. JohnValeron (talk) 17:57, 6 January 2014 (UTC)

There's an article called South Sudanese conflict (2013–present). Now that the early disclosures have been split off into History of the global surveillance disclosure, having "2013–present" in the title here would accurately indicate what's in the tin. —rybec 14:09, 7 January 2014 (UTC)

While I opposed inserting "2013-2014" at the beginning of the title, I **agree** with Rybec's suggestion to add "(2013–present)" at the end of the title. This approach is better because it demarcates a chronological starting point for the article without limiting its terminal point. JohnValeron (talk) 15:51, 7 January 2014 (UTC)

I could live with that as well.- MrX 16:50, 7 January 2014 (UTC)

Full support from me. **petrarchan47tc** 22:41, 7 January 2014 (UTC)

New sources

- "Officials' defenses of NSA phone program may be unraveling (http://www.washingtonpost.com/world/national-security/officials-defenses-of-nsa-phone-program-may-be-unraveling/2013/12/19/6927d8a2-68d3-11e3-ae56-22de072140a2_story.html)." *Washington Post*. December 19, 2013.

WhisperToMe (talk) 21:23, 20 December 2013 (UTC)

How GCHQ Monitors Germany, Israel and the EU

Spiegel Online (<http://www.spiegel.de/international/world/snowden-documents-show-gchq-targeted-european-and-german-politicians-a-940135.html>) By Laura Poitras, Marcel Rosenbach and Holger Stark; December 20, 2013
petrarchan47tc 03:00, 21 December 2013 (UTC)

NSA Reportedly Paid A Security Firm Millions To Ship Deliberately Flawed Encryption Technology

- Reuters (Cached) (http://webcache.googleusercontent.com/search?espv=210&es_sm=93&q=cache%3Awww.reuters.com%2Farticle%2F2013%2F12%2F20%2Fus-usa-security-rsa-idUSBRE9BJ1C220131220&oq=cache%3Awww.reuters.com%2Farticle%2F2013%2F12%2F20%2Fus-usa-security-rsa-idUSBRE9BJ1C220131220&gs_l=serp.3...1389.1389.0.1529.1.1.0.0.0.62.62.1.1.0....0...1c.1.32.serp..1.0.0.BvDxBqw8cGg)
- Reuters (<http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220>) By Joseph Menn; December 20,2013
- TechCrunch (<http://techcrunch.com/2013/12/20/nsa-reportedly-paid-a-security-firm-millions-to-ship-deliberately-flawed-encryption-technology/>) by Alex Wilhelm; December 20, 2013

petrarchan47tc 03:52, 21 December 2013 (UTC)

N.S.A. Spied on Allies, Aid Groups and Businesses

NYT (<http://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html>) By JAMES GLANZ and ANDREW W. LEHREN; December 21, 2013

petrarchan47tc 03:56, 21 December 2013 (UTC)

2013 in Review: The Year the NSA Finally Admitted Its "Collect It All" Strategy

They're probably already here, but just in case, a helpful list from EFF (<https://www.eff.org/deeplinks/2013/12/2013-year-nsas-collect-it-all-strategy-was-revealed>). **petrarchan47tc** 03:14, 27 December 2013 (UTC)

Additional new sources

- Neumeister, Larry. "Federal judge rules NSA phone surveillance legal (<http://www.chron.com/business/technology/article/Federal-judge-rules-NSA-phone-surveillance-legal-5096126.php?cmpid=hpbn>)." *Associated Press* at the

Houston Chronicle. December 27, 2013.

- "Greenwald: US, British media are servants of security apparatus (<http://rt.com/news/greenwald-snowden-nsa-hackers-conference-889/>). (Archive (<http://archive.is/CSJNd>)) *Russia Today*. December 27, 2013.

WhisperToMe (talk) 12:44, 28 December 2013 (UTC)

NSA capabilities with its TAO

There's more stuff about the NSA Office of Tailored Access Operations (TAO) and other NSA stuff:

- "Inside TAO: Documents Reveal Top NSA Hacking Unit (<http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>)." *Der Spiegel*. December 29, 2013.
- Appelbaum, Jacob, Judith Horchert and Christian Stöcker. "Shopping for Spy Gear: Catalog Advertises NSA Toolbox (<http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>)." *Der Spiegel*. December 29, 2013.
- "Report: NSA Intercepting Laptops Ordered Online, Installing Spyware (<http://www.forbes.com/sites/erikkain/2013/12/29/report-nsa-intercepting-laptops-ordered-online-installing-spyware/>)." *Forbes*. December 29, 2013.

I'm glad German newspapers are publishing articles in English. WhisperToMe (talk) 02:47, 30 December 2013 (UTC)

DROPOUTJEEP

NSA Reportedly Has Total Access To The Apple iPhone (<http://www.forbes.com/sites/erikkain/2013/12/30/the-nsa-reportedly-has-total-access-to-your-iphone/>) FORBES; By Erin Kain; 12.30.13

Includes video of Jacob Applebaum at the Chaos Communication Congress expanding on the NSA's abilities.

"And even the Apple iPhone — one of the most popular handheld devices in the world — can be exploited by the NSA, according to one of the classified documents, to let officials surreptitiously take pictures with the mobile's camera or stealthy turn on its microphone, access text messages or listen to voicemail." **petrarchan47**tc 05:15, 1 January 2014 (UTC)

DROPOUTJEEP may be in need of creation, if there is enough RS. **petrarchan47**tc 23:25, 15 January 2014 (UTC)

ACLU sues US government

- "ACLU sues US government over NSA spying (<http://www.bbc.co.uk/news/technology-25559056>)." *BBC*. 31 December 2013.

WhisperToMe (talk) 10:24, 1 January 2014 (UTC)

Proposal to remove references not publicly available.

I wanted to verify the information listed in reference 111 but found that the link requires a WSJ login. I'm not sure if policy permits such links as references but either way I propose removing such links, find alternatives or remove the content which can't be verified. Sephiroth storm (talk) 04:39, 5 January 2014 (UTC)

Wikipedia explicitly allows references behind paywalls, though it's preferable to get refs without paywalls. However you can verify info by asking the friendly folks at Wikipedia:RX for the source. They'll send you a personal copy.

WhisperToMe (talk) 11:02, 5 January 2014 (UTC)

Thanks for the info. Sephiroth storm (talk) 13:57, 5 January 2014 (UTC)

Section clarification.

I don't understand this: "Even if there is no reason to suspect U.S. citizens the CIA's National Counterterrorism Center is allowed to examine the government files of for possible criminal behavior. Previously the NTC was barred to do so, unless a person was a terror suspect or related to an investigation."

The first part is unclear. If there is no reason to suspect a target is a US Citizen? The CIA and the NSA are both primarily focused on Non US citizens so it makes sense to target non US persons. Who exactly are you talking about? "is allowed to examine the government files of for possible criminal behavior." - government files of what? what files? A database, a system, what files? "unless a person was a terror suspect or related to an investigation." What other reason would the files be accessed? Do we have reporting of the files being accessed for individuals who were not terror suspects or related to an investigation? I'd normally access the reference myself to see but, look above. Sephiroth storm (talk) 04:46, 5 January 2014 (UTC)

Even though the NSA's charter is that it should only collect data on foreigners, it is also collecting data on US citizens in its mass surveillance efforts. The agency says that it is not intentional with US citizens but there is a lot of controversy about it. WhisperToMe (talk) 15:11, 5 January 2014 (UTC)

How the NSA Threatens National Security

From *The Atlantic* today: How the NSA Threatens National Security (<http://www.theatlantic.com/technology/archive/2014/01/how-the-nsa-threatens-national-security/282822/>).

"U.S. government surveillance is not just about the NSA. The Snowden documents have given us extraordinary details about the NSA's activities, but we now know that the CIA, NRO, FBI, DEA, and local police all engage in ubiquitous surveillance using the same sorts of eavesdropping tools, and that they regularly share information with each other."

"We have no evidence that any of this surveillance makes us safer". **petrarchan47**^{tc} 01:25, 7 January 2014 (UTC)

Former NSA whistleblowers plead for chance to brief Obama on agency abuses

The letter: is here (<http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong/>)

"A group of former National Security Agency insiders who went on to become whistleblowers have written a letter to President Barack Obama, requesting a meeting with him to offer “a fuller picture” of the spy agency’s systemic problems.

The group of four intelligence specialists - William Binney, Thomas Drake, Edward Loomis and Kirk Wiebe - who worked at the NSA for “a total of 144 years, most of them at senior levels” stressed in the letter the need for Obama to address what they’ve seen as abuses that violated Americans’ Fourth Amendment rights and that have made proper, effective intelligence gathering more difficult.

“What we tell you in this Memorandum is merely the tip of the iceberg,” the group, calling themselves the Veteran Intelligence Professionals for Sanity (VIPS), wrote. “We are ready – if you are – for an honest conversation. That NSA’s bulk collection is more hindrance than help in preventing terrorist attacks should be clear by now despite the false claims and dissembling.”

The group criticized the NSA for its vast data collection policies, which they say bars the agency from effectively tracking actual terror plots in advance, such as the Boston Marathon bombing in April 2012." From RT (<http://rt.com/usa/nsa-obama-whistleblowers-letter-337/>). **petrarchan47**^{tc} 00:05, 9 January 2014 (UTC)

N.S.A. Devises Radio Pathway Into Computers

Latest leak: N.S.A. Devises Radio Pathway Into Computers (<http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html>) New York Times; By DAVID E. SANGER and THOM SHANKERJAN. January 14, 2014 **petrarchan47**tc 09:13, 15 January 2014 (UTC)

NSA collects millions of text messages daily in 'untargeted' global sweep

Latest from the Guardian (<http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>):

- NSA extracts location, contacts and financial transactions
- Dishfire program sweeps up 'pretty much everything it can'
- GCHQ using database to search metadata from UK numbers

petrarchan47tc 20:04, 16 January 2014 (UTC)

Broken Redirect

Dishfire redirects here, yet the page makes no mention of it whatsoever 108.182.88.129 (talk) 22:08, 16 January 2014 (UTC)

There's a new page created for it here -A1candidate (talk) 22:34, 16 January 2014 (UTC)

Orphaned references in Global surveillance disclosures (2013–present)

I check pages listed in Category:Pages with incorrect ref formatting to try to fix reference errors. One of the things I do is look for content for orphaned references in wikilinked articles. I have found content for some of Global surveillance disclosures (2013–present)'s orphans, the problem is that I found more than one version. I can't determine which (if any) is correct for *this* article, so I am asking for a sentient editor to look it over and copy the correct ref content into this article.

Reference named "bbc":

- From Egypt: "Country profiles: Egypt" (http://news.bbc.co.uk/1/hi/world/middle_east/country_profiles/737642.stm#media). BBC News. 2013-01-15. Retrieved 2013-02-08.
- From 2013: Walker, Andrew (7 December 2013). "WTO agrees global trade deal worth \$1tn" (<http://www.bbc.co.uk/news/business-25274889>). BBC News. Retrieved 7 December 2013.
- From Sri Mulyani Indrawati: "Indonesia finance minister resigns for World Bank post" (<http://news.bbc.co.uk/2/hi/asia-pacific/8661476.stm>). *BBC News*. May 5, 2010.
- From Julian Assange: "WikiLeaks: Swiss bank shuts Julian Assange's account" (<http://www.bbc.co.uk/news/world-11929034>). *BBC News*. 6 December 2010.
- From Tony Abbott: "Australia heads for hung parliament" (<http://www.bbc.co.uk/news/world-asia-pacific-11048968>). BBC. 21 August 2010. Retrieved 21 August 2010.
- From Australia: "Country profile: Australia" (<http://news.bbc.co.uk/2/hi/1250188.stm>). *BBC News*. 13 October 2009. Retrieved 7 April 2010.
- From Angela Merkel: "Bank uncertainty hits UK shares" (<http://news.bbc.co.uk/1/hi/business/7654182.stm>). *BBC*. 6 October 2008. Archived (<https://web.archive.org/web/20081007064831/http://news.bbc.co.uk/1/hi/business/7654182.stm>) from the original on 7 October 2008. Retrieved 6 October 2008.
- From United Kingdom: "Vertigo is named 'greatest film of all time'" (<http://www.bbc.co.uk/news/entertainment-arts-19078948>). *BBC News*. 2 August 2012. Retrieved 18 August 2012.
- From Dishfire: "Report: NSA 'collected 200m texts per day'" (<http://www.bbc.co.uk/news/world-us-canada-25770313>). BBC. Retrieved 16 January 2014.
- From Jay Carney: Connolly, Katie (January 28, 2011). "James Carney: Profile of White House press secretary" (<http://www.bbc.co.uk/news/world-us-canada-12304141>). *BBC News*. Retrieved January 28, 2011.

I apologize if any of the above are effectively identical; I am just a simple computer program, so I can't determine whether minor differences are significant or not. AnomieBOT ✉ 23:55, 16 January 2014 (UTC)

Invitation to help craft a proposal

Surveillance awareness day is a proposal for the English Wikipedia to take special steps to promote awareness of global surveillance on February 11, 2014. That date is chosen to coincide with similar actions being taken by organizations such as Mozilla, Reddit, and the Electronic Frontier Foundation.

Feedback from editors of this article would be greatly appreciated. Please come join us as we brainstorm, polish, and present this proposal to the Wikipedia Community. --HectorMoffet (talk) 12:24, 18 January 2014 (UTC)

Reactions of political leaders

I'm not comfortable with the "Reactions of political leaders" section. It feels like editorializing on our part, placing out of context quotes after a barrage of factual disclosures, with the reader inferring obliqueness from the leaders as a result. The quotes date from different times and do not reflect the ongoing narrative structure of the rest of the article. We would be better served by offering a brief summary of their reactions, like the succeeding paragraph. Gareth E Kegg (talk) 00:33, 29 January 2014 (UTC)

Retrieved from "http://en.wikipedia.org/w/index.php?title=Talk:Global_surveillance_disclosures_(2013–present)&oldid=592882483"

Categories: Start-Class Mass surveillance articles | High-importance Mass surveillance articles
 | Start-Class Espionage articles | High-importance Espionage articles | B-Class politics articles
 | Mid-importance politics articles | WikiProject Politics articles | B-Class United States articles
 | B-Class United States articles of Mid-importance | Mid-importance United States articles
 | B-Class United States Government articles | Unknown-importance United States Government articles
 | WikiProject United States Government articles | WikiProject United States articles
 | B-Class Politics of the United Kingdom articles | Mid-importance Politics of the United Kingdom articles

-
- This page was last modified on 29 January 2014 at 00:33.
 - 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.