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 Försvarsmyns 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*
<table>
<thead>
<tr>
<th>Program</th>
<th>International contributors and/or partners</th>
<th>Commercial partners</th>
</tr>
</thead>
</table>
| **PRISM** | - 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] | Microsoft[^30][^48][^49] |
| **XKeyscore** | - Bundesnachrichtendienst (BND) of Germany[^5][^50]  
- Bundesamt für Verfassungsschutz (BfV) of Germany[^5][^50]  
- Försvarets radioanstalt (FRA) of Sweden[^51][^52] | |
| **Tempora** | - National Security Agency (NSA)[^53][^54] | British Telecommunications (codenamed "Remedy")[^55]  
Interoute (codenamed "Streetcar")[^55]  
Level 3 (codenamed "Little")[^55]  
Global Crossing (codenamed "Pinnacle")[^55]  
Verizon Business (codenamed "Dacron")[^55]  
Viatel (codenamed "Vitreous")[^55]  
Vodafone Cable (codenamed "Gerontic")[^55] |
| **Muscular** | - NSA[^56] | |
| **Project 6** | - Central Intelligence Agency (CIA)[^57] | |
| **Stateroom** | - DSD[^58][^59]  
- Communications Security | |
The Mira hotel in Hong Kong, where Edward Snowden hosted his first meeting with Glenn Greenwald, Laura Poitras, and journalist Ewen MacAskill of The Guardian.

Establishment Canada (CSEC)\(^{[59][60]}\)
- GCHQ\(^{[59][61]}\)
- Special Collection Service (SCS)\(^{[59]}\)

<table>
<thead>
<tr>
<th>Lustre</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA(^{[63][64]})</td>
</tr>
<tr>
<td>France(^{[63][64]})</td>
</tr>
</tbody>
</table>

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, while Australia and New Zealand have been involved in the joint operation of the NSA's global analytical system **XKeyscore**. 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)
- The Shoal Bay Receiving Station near Darwin, Australia, is operated by the Australian Signals Directorate (ASD)
- The Australian Defence Satellite Communications Station near Geraldton, Australia, is operated by the ASD
- HMAS Harman outside Canberra, Australia, is operated by the ASD
- Waihopai Station near Blenheim, New Zealand, is operated by New Zealand's Government Communications Security Bureau (GCSB)

According to Edward Snowden, the NSA has established secret intelligence partnerships with many Western governments. 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.

In an interview published by *Der Spiegel*, Snowden accused the NSA of being "in bed together with the
The NSA granted the German intelligence agencies BND (foreign intelligence) and BfV (domestic intelligence) access to its controversial XKeyscore system. 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. 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. In December 2012 alone, the BND handed over 500 million metadata records to the NSA.

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.

According to an NSA document dated April 2013, Germany has now become the NSA's "most prolific partner". 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."

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. Both surveillance programs are "not identical".

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. 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.”

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".

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.

Snowden also confirmed that Stuxnet was cooperatively developed by the United States and Israel. 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."
On July 10, 2013, The Washington Post published a powerpoint presentation about the FAA702 Operations of the NSA, attributed to its Special Source Operations, in which NSA agents are tasked with the collection of communications from the following two sources:

1. **Upstream** – Under the first type of collection, data en route to its final destination would be intercepted via FAIRVIEW, STORMBREW, BLARNEY, and OAKSTAR.

2. **PRISM** – Under the second type of collection, data that has already reached its final destination would be directly harvested from the servers of the following U.S. service providers: Microsoft, Yahoo!, Google, Facebook, Paltalk, AOL, Skype, YouTube, and Apple Inc.

### 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. 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. 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. 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]
As part of disclosures about the XKeyscore surveillance tool, The Guardian released a classified NSA powerpoint slide explaining the importance of monitoring the HTTP (Hypertext Transfer Protocol) usage of "typical" Internet users. Notice the orange bar on top with the following line of text: "TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL". This is used to indicate that the presentation is a top secret document about communications intelligence (COMINT) that is shared among the "Five Eyes" of the United States, Australia, Canada, Great Britain, and New Zealand.

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]
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. 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]
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 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 "SIGNT 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, Brasilia, 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 access, many of them located within the United States.

- **FORSAT** — 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 SIGNT 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) 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.”

However federal judge William H. Pauley III in New York City ruled 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.

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.

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.

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. 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. 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."
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, The Guardian and ProPublica 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 videos watched daily as well as some user information for analysis purposes.\[167]\[311]\[312]

**User Activity Leads**

- Examine settings of phone as well as service providers for geo-location; specific to a certain region
- Networks connected
- Websites visited
- Buddy Lists
- Documents Downloaded
- Encryption used and supported
- User Agents

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]\n
**Aftermath**

*Main article: Aftermath of the global surveillance disclosure*
Reactions of political leaders

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

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.

2007 Memos by Michael Mukasey requesting Broader powers.


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

FY 2013 Intelligence Budget, additional tables

NSA presentations
Documents relating to spying on the 2009 G20 Summit

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.
Contact graph.

Hops in a contact graph.

2 hop contact graph.

Spying against Enrique Peña Nieto and his associates.

Details of the process in the Nieto operation.

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)

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. Documents classified as ECI contain the actual identities of the following NSA commercial partners operating the global surveillance network: Artifice, Lithium and Serenade. The name of a commercial NSA partner facility known as Steelknight is classified ECI and therefore not revealed in Snowden's documents.

Comparison with previous leaks
<table>
<thead>
<tr>
<th>Year</th>
<th>Disclosure</th>
<th>Size</th>
<th>Main source(s)</th>
<th>Major publisher(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1971</td>
<td>Pentagon Papers</td>
<td>4,100 pages</td>
<td>Daniel Ellsberg</td>
<td>The New York Times</td>
</tr>
</tbody>
</table>

See also

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

References


Global surveillance disclosures (2013–present) - Wikipedia, the ...  


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  


31. ^ Andy Greenberg (6/05/2013)., "NSA’s Verizon Spying Order Specifically Targeted Americans, Not Foreigners" (http://www.forbes.com/sites/andygreenberg/2013/06/05/vas-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."


Global surveillance disclosures (2013–present) - Wikipedia, the ...


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"


56. \(^{a b c d e f g h i j k l m}\) 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.


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.


Global surveillance disclosures (2013–present) - Wikipedia, the ...


Global surveillance disclosures (2013–present) - Wikipedia, the ...  


Global surveillance disclosures (2013–present) - Wikipedia, the ... http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(...


Global surveillance disclosures (2013–present) - Wikipedia, the ... http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(...


258. "Cold War treaty confirms Sweden was not neutral" (http://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-neutral). The Local. Retrieved 12 December 2013.


Global surveillance disclosures (2013–present) - Wikipedia, the ...

http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(...


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


Global surveillance disclosures (2013–present) - Wikipedia, the ...  


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


334. ^ Andrei Soldatov (8 January 2014), ИТОГИ ГОДА. СПЕЦСЛУЖБЫ (http://www.ej.ru/?a=note& id=24044) ежедневный журнал


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.


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.


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.


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.


(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.


Categories: Global surveillance
Talk:Global surveillance disclosures (2013–present)

From Wikipedia, the free encyclopedia

<table>
<thead>
<tr>
<th>This is the talk page for discussing improvements to the Global surveillance disclosures (2013–present) article.</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ This is not a forum for general discussion of the article's subject.</td>
</tr>
<tr>
<td>■ Please sign and date your posts by typing four tildes (----).</td>
</tr>
<tr>
<td>■ New to Wikipedia? Welcome! Ask questions, get answers.</td>
</tr>
<tr>
<td>■ Be polite, and welcoming to new users</td>
</tr>
<tr>
<td>■ Assume good faith</td>
</tr>
<tr>
<td>■ Avoid personal attacks</td>
</tr>
<tr>
<td>■ For disputes, seek dispute resolution</td>
</tr>
<tr>
<td>Article policies</td>
</tr>
<tr>
<td>■ No original research</td>
</tr>
<tr>
<td>■ Neutral point of view</td>
</tr>
<tr>
<td>■ Verifiability</td>
</tr>
</tbody>
</table>

This article is of interest to the following WikiProjects:

WikiProject Mass surveillance  (Rated Start-class, High-importance)

Global surveillance disclosures (2013–present) is within the scope of WikiProject Mass surveillance, which aims to improve Wikipedia's coverage of mass surveillance and mass surveillance-related topics. If you would like to participate, visit the project page, or contribute to the discussion.

Start  This article has been rated as Start-Class on the quality scale.

High  This article has been rated as High-importance on the importance scale.

WikiProject Espionage  (Rated Start-class, High-importance)

Global surveillance disclosures (2013–present) is within the scope of WikiProject Espionage, which aims to improve Wikipedia's coverage of Espionage and Espionage-related topics. If you would like to participate, visit the project page, or contribute to the discussion.

Start  This article has been rated as Start-Class on the quality scale.

High  This article has been rated as High-importance on the importance scale.

WikiProject Politics  (Rated B-class, Mid-importance)

This article is within the scope of WikiProject Politics, a collaborative effort to improve the coverage of politics 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 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**

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

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:**


**Funk**

Here are some **tasks you can do**:  
- **Article requests**: Bring Federal government of the United States to GA.  
- **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  
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/wiki/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/wiki/index.php?title=Global_surveillance_disclosure&diff=prev&oldid=583602404]) on 00:48, 28 November 2013. The former page's history ([en.wikipedia.org/wiki/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.

Text from this version ([en.wikipedia.org/wiki/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/wiki/index.php?title=Global_surveillance_disclosure&diff=prev&oldid=588625542]) on 2014-01-01T06:09:59. The former page's history ([en.wikipedia.org/wiki/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.
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":

Reference named "WP20130830":


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. petrarchan47te 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. petrarchan47tc 23:15, 18 December 2013 (UTC)

More sources


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


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


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

**Merkel-Obama meeting**


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

**EU parliament meeting**


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 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 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
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.

petrarchan47te 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.

petrarchan47te 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.

petrarchan47te 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.

petrarchan47te 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 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] 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)
New sources


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

How GCHQ Monitors Germany, Israel and the EU

Spielgel 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=cach%3Awww.reuters.com%2Farticle%2F2013%2F12%2F20%2Fus-usa-security-rsa-idUSBRE9BJ1C220131220&cc=us&sa=X&q=cache%3Awww.reuters.com%2Farticle%2F2013%2F12%2F20%2Fus-usa-security-rsa-idUSBRE9BJ1C220131220&gs_l=serp.3...1389.1389.0.1529.1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.c.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


petrarchan47tc 03:52, 21 December 2013 (UTC)

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


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


NSA capabilities with its TAO

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


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." petrarchan47tc 05:15, 1 January 2014 (UTC)

DROPOUTJEEP may be in need of creation, if there is enough RS. petrarchan47tc 23:25, 15 January 2014 (UTC)

ACLU sues US government


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


"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". petrarchan47tc 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/). petrarchan47tc 00:05, 9 January 2014 (UTC)

N.S.A. Devises Radio Pathway Into Computers

**NSA collects millions of text messages daily in '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":

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)