BUSINESS INSIDER
DEUTSCHLAND

This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks

PAUL SZOLDRA
16.09.2016, 14:00

Handout/Getty Images

In June 2013, The Guardian reported the first leak based on top-secret documents that then 29-year-old Edward Snowden stole from the National Security Agency. At the time, Snowden worked as an intelligence contractor for Booz Allen Hamilton in Hawaii.

That leak would certainly not be the last. In the years since, journalists have released more than 7,000 top-secret documents that Snowden entrusted them with, which some believe is less than 1% of the entire archive.

Now, with the film "Snowden" premiering Friday, it's worth taking a look back at what secrets Snowden actually revealed. We've compiled every single leak that came out in the first year of the Snowden saga, though there were many more that came later.

Snowden downloaded up to 1.5 million files, according to national intelligence officials, before jetting from Hawaii to Hong Kong to meet with journalists Glenn Greenwald and Laura Poitras. After he handed off his treasure trove of documents, he flew from Hong Kong and later became stranded in Moscow. His future was far from certain, as the journalists he trusted started revealing his secrets.

Here is everything that Snowden's leaks revealed between 2013 and 2014:

• With a top-secret court order, the NSA collected the telephone records from millions of Verizon customers. — June 6, 2013

• The NSA accessed and collected data through back doors into US internet companies such as Google and Facebook with a program called Prism. — June 7, 2013

• An 18-page presidential memo shows Obama ordering intelligence officials to draw up a list of overseas targets for cyberattacks. — June 7, 2013   asdf
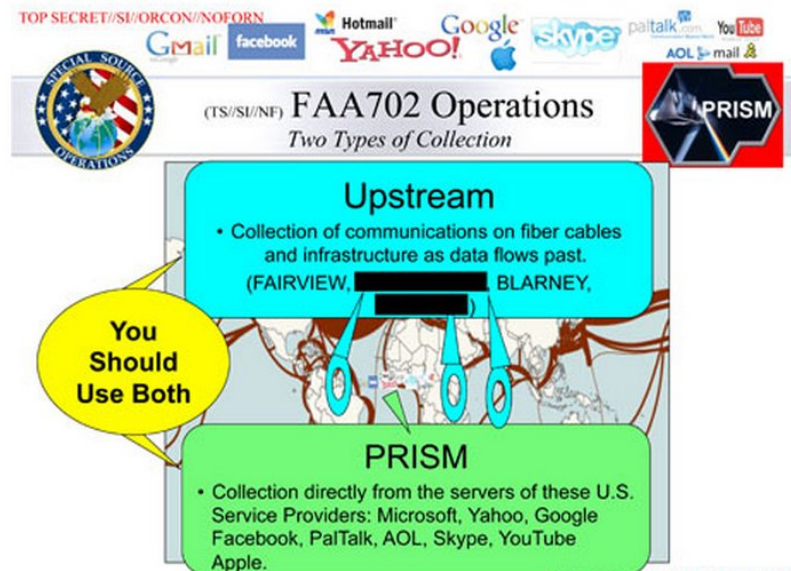
The Guardian

• Documents reveal
the NSA's Boundless Informant program, which gives the agency near real-time ability to understand how much intelligence coverage there is on certain areas through use of a "heat map." — June 8, 2013

• The NSA was hacking computers in Hong Kong and mainland China, few of which were military systems. — June 13, 2013

• Britain's GCHQ (its intelligence agency) intercepted phone and internet communications of foreign politicians attending two G-20 meetings in London in 2009. — June 16, 2013

• Top-secret procedures show steps the NSA must take to target and collect data from "non-US persons" and how it must minimize data collected on US citizens. — June 20, 2013

• Britain's GCHQ taps fiber-optic cables to collect and store global email messages, Facebook posts, internet histories, and calls, and then shares the data with the NSA. — June 21, 2013

• The NSA has a program codenamed EvilOlive that collects and stores large quantities of Americans' internet metadata, which contains only certain information about online content. Email metadata, for example, reveals the sender and recipient addresses and time but not content or subject. — June 27, 2013

• Until 2011, the Obama administration permitted the NSA's continued collection of vast amounts of Americans' email and internet metadata under a Bush-era program called Stellar Wind. — June 27, 2013

• The US government bugged the offices of the European Union in New York, Washington, and Brussels. — June 29, 2013

• The US government spies on at least 38 foreign embassies and missions, using a variety of electronic surveillance methods. — June 30, 2013

• The NSA spies on millions of phone calls, emails, and text messages of ordinary German citizens. — June 30, 2013

• Using a program called Fairview, the NSA intercepts internet and phone-call data of Brazilian citizens. — July 6, 2013

• Monitoring stations set up in Australia and New Zealand help feed data back to NSA's XKeyscore program. — July 6, 2013

• The NSA conducts surveillance on citizens in a number of Latin American countries, including Venezuela, Colombia, Argentina, Panama, Ecuador, Peru, and others. The agency also sought information on oil, energy, and trade. — July 9, 2013

• The Washington Post publishes a new slide detailing NSA's "Upstream" program of collecting communications from tech companies through fiber-optic cables to then feed into its Prism database. — July 10, 2013

• Germany's Federal Intelligence Service, BND, helps contribute data to the NSA's XKeyscore program. — July 20, 2013

asdf

The Guardian
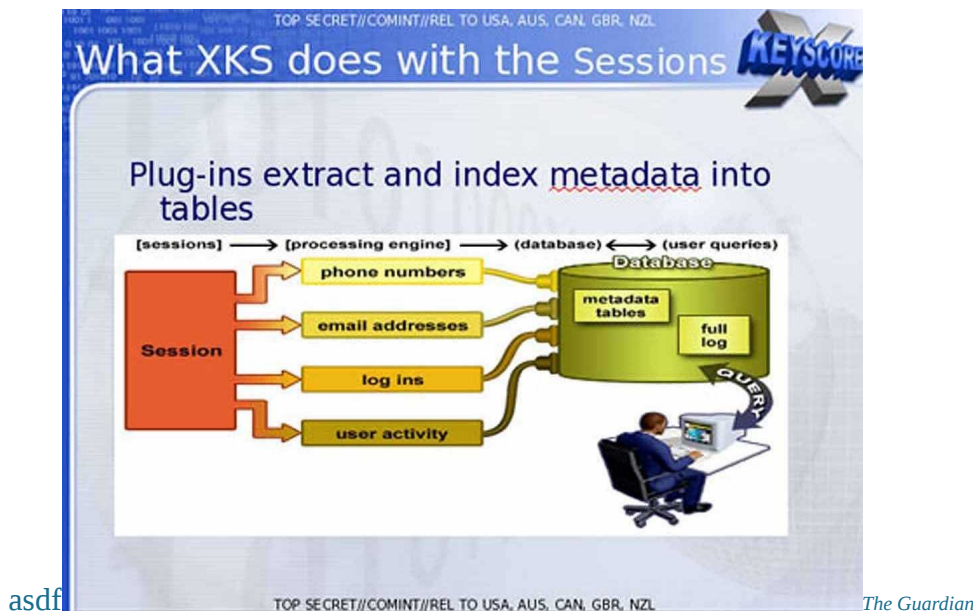
• NSA analysts, using the XKeyscore program, can search through enormous databases of emails, online chats, and browsing histories of targets. — July 31, 2013

• The US government paid Britain's GCHQ roughly $155 million over three years to gain access and influence over its spying programs. — August 1, 2013

• Seven of the world's leading telecommunications companies provide GCHQ with secret, unlimited access to their network of undersea cables. — August 2, 2013

• The NSA provided surveillance to US diplomats in order to give them the upper hand in negotiations at the UN Summit of the Americas. — August 2, 2013

• The NSA sifts through vast amounts of Americans' email and text communications going in and out of the country. — August 8, 2013

• Internal NSA document reveals an agency "loophole" that allows a secret backdoor for the agency to search its databases for US citizens' emails and phone calls without a warrant. — August 9, 2013

• NSA collection on Japan is reportedly maintained at the same priority as France and Germany. — August 12, 2013

• The NSA broke privacy rules thousands of times per year, according to an internal audit. — August 15, 2013

• NSA analysts revealed to have sometimes spied on love interests, with the practice common enough to have coined the term LOVEINT, or love intercepts. (It was unclear whether this report came from

Snowden docs.) — August 23, 2013

• Britain runs a secret internet-monitoring station in the Middle East to intercept emails, phone calls, and web traffic, The Independent reports, citing Snowden documents. Snowden denies giving The Independent any documents, alleging the UK government leaked them in an attempt to discredit him. — August 23, 2013

• The top-secret US intelligence "black budget" is revealed for 2013, with 16 spy agencies having a budget of $52.6 billion. — August 29, 2013
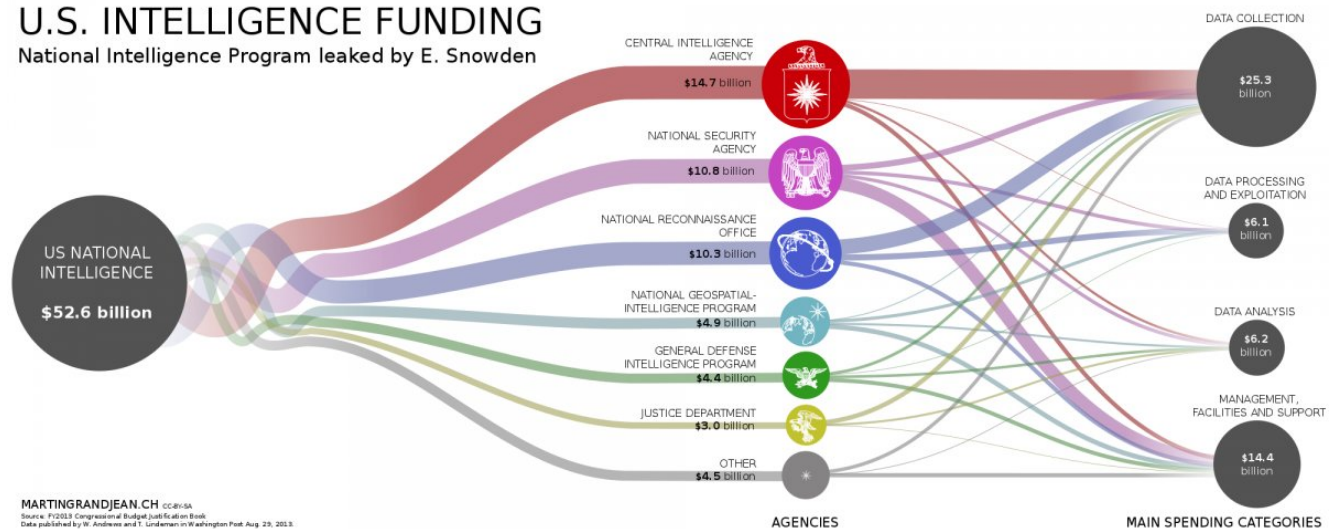

Martin Grandjean

• Expanding upon data gleaned from the "black budget," the NSA is found to be paying hundreds of millions of dollars each year to US companies for access to their networks. — August 29, 2013

• The US carried out 231 offensive cyberattacks in 2011. — August 30, 2013

• The NSA hacked into Qatar-based media network Al Jazeera's internal communications system. — August 31, 2013

• The NSA spied on former Brazilian President Dilma Rousseff and Mexican President Enrique Peña Nieto (then a candidate). — September 1, 2013

• Using a "man in the middle" attack, NSA spied on Google, the French Ministry of Foreign Affairs, the Society for Worldwide Interbank Financial Telecommunications, and the Brazilian oil company Petrobras. — September 2, 2013

• A US intelligence "black budget" reveals Al Qaeda's effort to jam, hack, and/or shoot down US surveillance drones. — September 3, 2013

• A joint investigation by ProPublica, The New York Times, and The Guardian finds the NSA is winning its war against internet encryption with supercomputers, technical know-how, and court orders. — September 5, 2013

• The NSA has the ability to access user data for most major smartphones on the market, including Apple iPhones, BlackBerrys, and Google Android phones. — September 7, 2013

• The NSA shares raw intelligence data (with information about American citizens) to Israel with an information-sharing agreement. — September 11, 2013

• The NSA monitors banks and credit institutions for a comprehensive database that can track the global flow of money. — September 16, 2013

• Britain's GCHQ launched a cyberattack against Belgacom, a partly state-owned Belgian telecommunications company. — September 20, 2013

• The NSA spies on Indian diplomats and other officials in an effort to gain insight into the country's nuclear and space programs. — September 23, 2013

• The NSA's internal "wiki" website characterizes political and legal opposition to drone attacks as part of "propaganda campaigns" from America's "adversaries." — September 25, 2013

• Since 2010, the NSA has used metadata augmented with other data from public, commercial, and other sources to create sophisticated graphs that map Americans' social connections. — September 28, 2013

• The NSA stores a massive amount of internet metadata from internet users, regardless of whether they are being targeted, for up to one year in a database called Marina. — September 30, 2013

• The NSA and GCHQ worked together to compromise the anonymous web-browsing Tor network. — October 4, 2013

• Canada's signals intelligence agency, CSEC, spied on phone and computer networks of Brazil's Ministry of Mines and Energy and shared the information with the "Five Eyes" intelligence services of the US, Canada, Britain, Australia, and New Zealand. — October 7, 2013
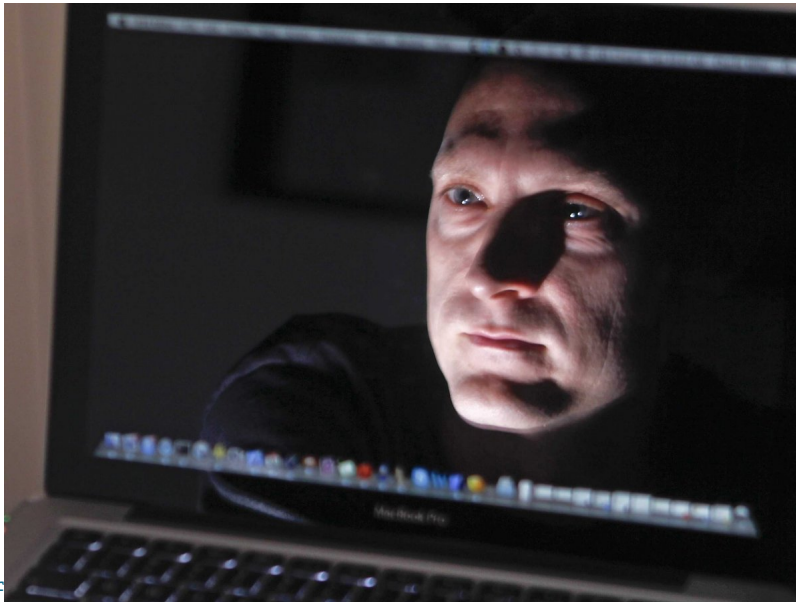
asdf

A reflection of Charlie Miller is pictured on his computer screen in his home-office in Wildwood, Missouri April 30, 2013. Miller is a security researcher at Twitter who previously worked for the National Security Agency (NSA).

REUTERS/Sarah Conard

• The NSA collected more than 250 million email contact lists from services such as Yahoo and Gmail. — October 14, 2013

• NSA surveillance was revealed to play a key role in targeting for overseas drone strikes. — October 16, 2013

• The NSA spied on French citizens, companies, and diplomats, and monitored communications at France's embassy in Washington and its UN office in New York. — October 21, 2013

• The NSA tapped the mobile phone of German Chancellor Angela Merkel. — October 23, 2013

• The NSA spied on Italian citizens, companies, and government officials. — October 24, 2013

• The NSA monitored the phone calls of 35 world leaders and encouraged other government agencies to share their "Rolodexes" of foreign politicians so it could monitor them. — October 25, 2013

• The NSA spied on Spanish leaders and citizens. — October 25, 2013

• The NSA stations surveillance teams at 80 locations around the world. — October 27, 2013

• A joint program between the NSA and Britain's GCHQ called Muscular infiltrates and copies data flowing out of Yahoo and Google's overseas data centers. One slide boasted of "SSL added and removed here!" with a smiley face. — October 30, 2013

• The NSA spied on the Vatican. (The Panorama website did not cite Snowden as the source.) — October 30, 2013

> One slide boasted of "SSL added and removed here!" with a smiley face.

• Australia's intelligence service has surveillance teams stationed in Australian embassies around Asia and the Pacific. — October 31, 2013

• One document reveals tech companies play a key role in NSA intelligence reports and data collection. — November 1, 2013

• Britain's GCHQ and other European spy agencies work together to conduct mass surveillance. — November 1, 2013

• Strategic missions of the NSA are revealed, which include combatting terrorism and nuclear proliferation, as well as pursuing US diplomatic and economic advantage. — November 2, 2013

• Australia's Defense Signals Directorate and the NSA worked together to spy on Indonesia during a UN climate change conference in 2007. — November 2, 2013

• The NSA spied on OPEC. — November 11, 2013

• GCHQ monitored the booking systems of 350 high-end hotels with a program called Royal Concierge, which sniffed for booking confirmations sent to diplomatic email addresses that would be flagged for further surveillance. — November 17, 2013

• Australia's DSD spied on the cellphones of top Indonesian officials, including the president, first lady, and several cabinet ministers. — November 18, 2013

• The NSA spied on millions of cellphone calls in Norway in one 30-day period. — November 19, 2013

• The British government struck a secret deal with the NSA to share phone, internet, and email records of UK citizens. — November 20, 2013

• A NSA strategy document reveals the agency's goal to acquire data from "anyone, anytime, anywhere" and expand its already broad legal powers. — November 22, 2013

• The NSA infected more than 50,000 computer networks worldwide with malware designed to steal sensitive information. — November 23, 2013

• The NSA gathers evidence of visits to pornographic websites as part of a plan to discredit Muslim jihadists. — November 26, 2013

• Working with Canadian intelligence, the NSA spied on foreign diplomats at the G-8 and G-20 summits in Toronto in 2010. — November 28, 2013

• The Netherlands' intelligence service gathers data on web-forum users and shares it with the NSA. — November 30, 2013

• A draft document reveals Australia offered to share information collected on ordinary Australian

asdf   REUTERS/Jason Reed

citizens with the NSA and other "Five Eyes" partners. — December 1, 2013

• The NSA siphons billions of foreign cellphone location records into its database. — December 4, 2013

• Widespread spying is revealed in Italy, with the NSA spying on ordinary Italians as well as diplomats and political leaders. — December 5, 2013

• Swedish intelligence was revealed to be spying on Russian leaders, then passing it on to the NSA. — December 5, 2013

• A document reveals the extent of the relationship between NSA and Canadian counterparts, which includes information-sharing and Canada allowing NSA analysts access to covert sites it sets up. — December 9, 2013

Blizzard

• Intelligence operatives with NSA and GCHQ infiltrate online video games such as "World of Warcraft" in an effort to catch and stop terrorist plots. — December 9, 2013

• Piggybacking on online "cookies" acquired by Google that advertisers use to track consumer preferences, the NSA is able to locate new targets for hacking. — December 10, 2013

• The NSA has the ability to decrypt the common A5/1 cellphone encryption cipher.

— December 13, 2013

• The NSA secretly paid the computer security firm RSA $10 million to implement a "back door" into its encryption. — December 20, 2013

• A document reveals how Britain's GCHQ spied on Germany, Israel, the European Union, and several nongovernmental organizations. — December 20, 2013

• With a $79.7 million research program, the NSA is working on a quantum computer that would be able to crack most types of encryption. — January 2, 2014

• Using radio transmitters on tiny circuit boards or USB drives, the NSA can gain access to computers not connected to the internet. — January 14, 2014

• The NSA scoops "pretty much everything it can" in untargeted collection of foreign text messages for its Dishfire database. — January 16, 2014

• The NSA scoops up personal data mined from smartphone apps such as Angry Birds. — January 27, 2014

• A GCHQ program called Squeaky Dolphin monitors YouTube, Facebook, and Blogger for "broad real-time monitoring of online activity." — January 27, 2014

> The NSA scoops "pretty much everything it can" in untargeted collection of foreign text messages.

• The NSA spied on negotiators during the 2009 UN climate change conference in Copenhagen, Denmark. — January 29, 2014

• CSEC, Canada's national cryptologic agency, tested a pilot program with the NSA that captured metadata from users who had logged into free airport Wi-Fi. — January 30, 2014

• Britain's GCHQ waged war on hacker groups such as Anonymous and Lulzsec, mounting Distributed Denial-of-Service attacks and infiltrating their chat rooms. — February 5, 2014

• The NSA reportedly monitored former German Chancellor Gerhard Schröder in the run-up to the Iraq war. — February 5, 2014

• Britain's GCHQ used "dirty tricks" such as computer viruses and sexual "honey traps" to target adversaries. — February 7, 2014

• The US's "targeted killing" program of drone strikes relies mostly on cellphone metadata and geolocation, rather than on-the-ground human intelligence. — February 10, 2014

• An American law firm was monitored by the Australian Signals Directorate while representing the government of Indonesia during a trade dispute. — February 15, 2014

• The NSA and Britain's GCHQ reportedly monitored traffic to the WikiLeaks website and considered a move to monitor communications going to or from WikiLeaks and the Pirate Bay. — February 18, 2014

• Britain's GCHQ conducts covert operations to disrupt and shape online discourse. — February 24, 2014

• Britain's GCHQ, using a program called Optic Nerve, intercepted and stored webcam images from millions of Yahoo users, then passed them on to the NSA's XKeyscore database. — February 28, 2014

• The NSA shared intelligence that helped the Dutch navy capture a ship hijacked by pirates off Somalia, and the Netherlands regularly shares information with the NSA regarding Somalia and Afghanistan. — March 5, 2014

• The NSA has an advice columnist similar to "Dear Abby" who writes an "Ask Zelda" column distributed on the agency's internal network. — March 7, 2014

• NSA developed sophisticated malware "implants" to infect millions of computers worldwide. In one example, the NSA posed as a fake Facebook server to infect a target's computer and steal files. — March 12, 2014   asdf

First Look/Trevor Paglen

• Document reveals that, while many foreign governments share information with NSA, few senior officials outside of the intelligence or defense sphere have any knowledge of it. — March 13, 2014

• The NSA built a system capable of recording "100%" of a foreign country's phone calls with a voice intercept program called Mystic. The Washington Post did not name the countries where the program was used. — March 18, 2014

• The NSA specifically targets foreign systems administrators to gain access to their networks. — March 20, 2014

• The NSA closely monitored the Chinese technology firm Huawei in attempt to reveal ties between the company and the Chinese military. The agency also spied on Chinese banks and other companies, as well as former President Hu Jintao. — March 22, 2014

• Malaysia's political leadership is a high-priority intelligence target for the US and Australia — March 30, 2014

• NSA and Britain's GCHQ discussed various methods of deception, use of propaganda, mass messaging, and pushing stories on social media sites — April 4, 2014

• The Norwegian Intelligence Service is developing a supercomputer, called Steel Winter, to decrypt and analyze data from Afghanistan, Russia, and elsewhere. — April 26, 2013

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Ars Technica

• Britain's GCHQ asked the NSA for "unsupervised access" to the NSA's vast databases. It was unclear whether the request was granted. — April 30, 2014

• The NSA physically intercepts routers, servers, and other computer networking equipment before it's exported outside the US, implants "back door" surveillance tools, then repackages them with a factory seal and ships them out. — May 12, 2014

• The NSA is intercepting, recording, and archiving virtually every cellphone call in the Bahamas and one other country, which The Intercept redacted. It also reveals metadata collection on Mexico, Kenya, and the Philippines. — May 19, 2014

• After giving journalist Glenn Greenwald a 72-hour warning to reveal the nation redacted from his previous report on mass surveillance of an entire country, WikLeaks reveals the country in question is Afghanistan. — May 23, 2014

• The NSA harvests millions of faces from web images for use in a previously undisclosed facial recognition database. — May 31, 2014

Author's note: I've tried my best to be thorough in sifting through the hundreds of leaks that have come to light thus far. I have not included Snowden's movements, legal situation, or any of the political drama surrounding the leaks. This timeline only shows the many reports stemming from documents the ex-NSA contractor handed over to journalists.

If I have missed any leaks in the hundreds of news stories on these items, that mistake is mine alone.

This post relied upon a similar timeline from Al Jazeera America, as well as a catalog at Lawfare Blog, and an article at the National Journal.