Glossary of NSA Key Terms
1.30.2014

Accumulo

The name given to an open-source database created by the National Security Agency (NSA) but later made available to others via the Apache Foundation. It stores large amounts of structured and unstructured data across many computers and can use it to create near real-time reports.

One of its key features is that users with different levels of clearance are shown different amounts of information. So a high-level operator might be shown all the data available, while a lower-level one would be restricted to seeing only certain columns, and might never be aware that other topics existed.

It was modelled on Google's BigTable system.

Angry Birds

Leaked documents, **published by ProPublica**, indicate that the NSA and GCHQ routinely try to gain access to personal data from Angry Birds and other mobile applications.

The **news site reports** that the two agencies have worked together since 2007 to obtain the details from mobile phones and tablet apps that send private information about their users over the internet.

The documents indicate that app transmissions can include details of age, gender, location and even sexual preference. The papers use Android apps in most of the provided examples, but state that data can be gathered from equivalent apps on other platforms.

However, ProPublica adds that the specifics of the data haul are not clear.

Ant

A division of the NSA that provides software and hardware surveillance products, **according to Der Spiegel**.

The German magazine **published extracts** from a leaked catalogue featuring a range of such implants.

Their codenames included:

- Cottonmouth - USB-based devices that offer agents wireless access to a target's network
- Deitybounce - technology that allows software to be installed on Dell's PowerEdge computer servers
- Dropoutjeep - software that allows voicemail, contact list, location, camera image capture and sound data to be captured from Apple iPhones
- Headwater - software that allows spyware to be covertly sent through selected routers manufactured by the Chinese firm Huawei
- Howlermonkey - a radio frequency transceiver that can be used to copy data or take control of a targeted computer
- Jetplow - firmware that creates a backdoor into certain Cisco firewall products
- Loudauto - a small listening device that uses very little power
- Monkeycalendar - software that takes location data from a mobile phone and secretly sends the details as text messages
- Somberknave - software that allows agents to take control of PCs running Windows XP

Appelbaum, Jacob

One of the journalists given direct access to some of Edward Snowden's leaked documents.

He has written articles for Germany's Der Spiegel magazine.

Mr Appelbaum is also known for developing security and encryption software, representing Wikileaks and serving as an advocate for the Tor Project.

Back-door access

The idea that cyberspies can access data held by organisations without having to formally ask them to hand it over through the "front door". This allows the bodies involved to be kept in the dark about the subject matter and amount of information being taken.

Initial reports following the early Prism revelations sparked speculation that the firms involved had provided agents with direct backdoor access to their servers - something they strongly denied. The Washington Post later reported that the NSA and the UK intelligence agency, GCHQ, were instead intercepting and copying data from the companies without their knowledge via a project **codenamed Muscular**.

The phrase back door has also been used to refer to allegations that the spy agencies had inserted secret vulnerabilities into **encryption software**.

If true, this would mean spies could overcome steps taken by service providers and their users to ensure that only the sender and receiver of a communication should be able to read it.

Belgacom

A Belgian telecoms provider whose customers include several EU institutions.

The firm revealed in September 2013 that its systems had been hacked since at least 2011.

Belgian newspaper **De Standaard initially reported** that the NSA was believed to be responsible.

However, Der Spiegel later said that leaked documents indicated **GCHQ had carried out the attack**, which had been codenamed Operation Socialist.

Blackfoot

The codename given to an NSA operation to gather data from French diplomats' offices at the United Nations in New York, according to leaked documents **reported by Der Spiegel**.

It says papers dated September 2010 indicated that information was collected from bugged computer screens.

Bluf

An acronym used by the US military for "bottom line up front", used to signal that only the key facts are being presented. It appears towards the top of some NSA documents ahead of briefing notes.

Boundless Informant

Documents **published by the Guardian** indicate this is a tool used by the NSA to analyse the metadata it holds. It aims to let analysts know what information is currently available about a specific country and whether there are trends can be deduced.

The newspaper says the agency uses "big data" analysis technology to scour the billions of pieces of intelligence held at any one time to provide "near real-time" details about available coverage.

A screenshot of the NSA's **alleged user interface** shows different countries colour-coded to indicate how much data is known about each one.

Buddy list

A list of people a user is connected to via an instant messaging service or other social network.

The spy agencies reportedly combine the information with data gathered from users' email address books **to map connections between targets**.

According to one leaked document, **published by the Washington Post**, the NSA collected about half a million buddy lists and webmail inbox details on "a representative day".

Bullrun

The name of a counter-encryption programme run by the NSA.

A document **published by the Guardian** says it uses a variety of processes, including "advanced mathematical techniques" and "industry relationships" to reveal an unscrambled version of the data.

Cheesy Name

A GCHQ program, **identified by the Guardian**, designed to identify encryption keys that could be cracked by the agency's computers.

Collection

Leaked documents refer to **four types** of NSA data collection with regard to US persons (a citizen of the country or someone located within its borders):

- Intentional - the deliberate targeting of an individual or group. NSA agents are forbidden from the intentional collection of data about US persons unless they are given special authority to do so.
- Inadvertent - information gathered about a person whom the agent believed to be foreign, but later learned to be a US person.
- Incidental - data gathered as a by-product of an inquiry into a legitimate foreign target, which might reveal information about a US person. An alleged memo, **dated March 2013**, says this does not constitute a violation and does not have to be reported for inclusion in reports to Congress.
- Reverse - the targeting of a foreign subject to intentionally gather information about a US person they are in contact with. NSA agents are banned from doing this and told to notify a supervisor if it occurs.
-

Cloud

The term used to refer to data stored at, or software run from, a service provider's data centres as opposed to being kept or processed on the user's own computer.

Many of the Snowden leaks detail the alleged efforts of the NSA and GCHQ to study information held in the cloud that their targets might have believed was protected from others' view.

Comint

An abbreviation for "communications intelligence".

Communications Security Establishment (CSEC)

Canada's codebreaking security agency.

Its logo featured in a leaked GCHQ document, **published by the Guardian**, which discussed the hacking of Blackberry devices at a G20 summit.

Computer Network Attack (CNA)

A term **used by the NSA** to refer to actions taken to "disrupt, deny, degrade, or destroy" information held on targeted computers and the computers themselves.

Computer Network Defence (CND)

A phrase **used by the NSA** to refer to computer-based actions taken to "protect, monitor, analyse, detect, and respond to network attacks, intrusions, disruptions, or other unauthorised actions".

Computer Network Exploitation (CNE)

The term **used by the NSA** to refer to efforts to exploit data gathered from its targets.

Conveyance

Identified **by an NSA slide,** the term appears to refer to a system used to remove voice content collected about US persons as part of the Prism programme before it is analysed by a process called Nucleon.

US persons - citizens of the country or someone located within its borders - are not supposed to be the subject of the agency's investigations.

Data Intercept Technology Unit (Ditu)

An FBI unit that **one of the leaked slides suggests** collects much of the data gathered from internet companies as part of the Prism programme, before passing it on to the NSA.

According to an **investigation by Foreign Policy magazine**, the operation is based at Marine Corps Base Quantico in Virginia, and acts as "the primary liaison" between the NSA and companies including Google, Facebook and Apple. The report says the unit maintains equipment that takes the desired information from the firms, and makes sure that any encryption processes used by them do not prevent the businesses from handing over data they have a legal responsibility to share.

The article adds that having the Ditu act as a conduit allows companies to report that they do not hand information "directly" to the NSA.

Data mining

Analysis of large stores of information in order to obtain new knowledge.

In the case of the US and UK spy agencies, the data mined is reported to include phone call records, emails, instant messages and other social network activity, photos and videos.

As time goes on, the challenge is that the data generated is growing at an exponential rate. **According to a forecast** by the magazine Popular Mechanics, the amount of data created in 2020 will be 50 times greater than a decade earlier.

Deep Packet Injection

The addition of data into an internet stream.

The technique has previously been used by some internet service providers (ISPs) to replace websites' adverts with their own.

The NSA and GCHQ are alleged to do it to send code to targets' computers that causes them to be infected with spyware as part of an operation codenamed QuantumInsert.

Deep Packet Inspection

Data sent over the internet is split into packets, each of which is identified by a header - containing information about where it is being sent, where it came from and what is contained.

Normally these headers are used to ensure data gets to where it is meant to go, and - when necessary - ensure a packet is re-sent if there was a problem with the original copy.

Deep packet inspection refers to a closer analysis of the contents of each packet. This might be done to detect malware or to obtain statistics about network activity. In addition, it can be used to spy on the communications.

According to documents leaked by Mark Klein - an ex-employee of phone network AT&T - to the **Electronic Frontier Foundation**, one of the machines used by the NSA to do deep packet inspection was a Narus Semantic Traffic Analyzer, built by a division of Boeing.

Mr Klein said that by the mid-2000s each machine could analyse 10GB worth of data packets and 2.5GB of web traffic or email every second.

Demultiplexer

The process used to split captured signals back into individual data streams. It is sometimes referred to as a "demux" tool.

One alleged NSA leak **makes reference to developing** "custom demultiplexers" so the agency could make use of data sourced from Yahoo. It said these used a proprietary data format called Narchive to transfer packages containing entire email accounts between Yahoo's servers.

Dewsweeper

A leaked NSA document **published by Le Monde** identifies this as a hardware device that provides wireless access to a device on a target's network when plugged into one of the machine's USB sockets.

Dial Number Recognition (DNR)

A term used by the NSA to refer to information gathered from telephone taps.

According to documents seen by Le Monde, the NSA collected 124.8 billion pieces of DNR data over the course of four weeks in 2013.

Digital Network Intelligence (DNI)

A term used by the NSA to refer to content sent across the internet. This includes everything from Skype voice calls to web page requests,

According to Le Monde, the NSA collected 97.1 billion pieces of DNI data over the course of four weeks in 2013.

Dishfire

The **NSA has confirmed** this is the codename for a system used to process and store SMS message data.

A leaked 2011 NSA presentation, **published by the Guardian**, indicated it was used to collect about 194 million texts a day, adding that the content was shared with GCHQ.

The documents said that GCHQ's agents should toggle an option to ensure they would not see UK content, which would be illegal to read without a warrant. The report added that US-related SMS messages were automatically hidden from NSA staff.

Further analysis of the data is said to be carried out by a related system named Prefer.

Dragnet

A term **used in somemedia reports** and by **civil liberty groups** to refer to the huge amount of information being trawled by the spy agencies.

Dropmire

The name for a way to bug security-enhanced fax machines, which was identified by a leaked document dated to 2007, **according to the Guardian**.

It indicates the technique provides the NSA with access to documents that have passed through encrypted fax machines based in other countries' foreign embassies.

Echelon

The codename given to a global intelligence-gathering network operated on behalf of the Five Eyes Alliance (Australia, Canada, New Zealand, UK and US).

A European Parliament report, **published in 2001**, suggests the first part of the network was built in 1971 and its focus was to intercept private and commercial - rather than military - communications.

The inquiry says that the system was alleged to be able to intercept any "telephone, fax, internet or email message sent by any individual".

Edgehill

A UK-run counter-encryption programme that is named after a battle fought in 1642 as part of the English Civil War.

The **Guardian reported that** the operation's focus in 2012 was to "understand" Hotmail, Google, Yahoo and Facebook's encryption techniques. It adds that by 2015 the agency aims to have cracked the codes used by 15 major internet companies.

EgotisticalGiraffe

The alleged codename given to an NSA effort to track users of Tor (The Onion Router) - a project that aims to let people browse the web anonymously by bouncing their traffic through other people's computers.

Documents **published by the Guardian** indicate the technique involves exploiting vulnerabilities that exist in a version of the Firefox browser that used to be included in the Tor Browser Bundle - a collection of programs pre-configured to let people use the service. The browser's developer, Mozilla, has fixed the flaws in later versions.

The **Washington Post added** that other leaked papers suggested the operation was used to unmask a "key propagandist" for the al-Qaeda terrorist organisation.

Encryption

The digital scrambling of source material, turning it into "ciphertext" - what appears to be a garbled stream of characters that is only supposed to become understandable if a piece of information called a "key" is used to turn it back into its original form.

In theory, if data is encrypted and the key is not shared, a third party should not be able to read it. Web browsers usually notify their users that what they are seeing has been encrypted/decrypted by showing a little padlock next to the web address.

The NSA openly states that part of its job is to counteract its adversaries' use of encryption.

"Terrorists, cybercriminals, human traffickers and others... use code to hide their activities. Our intelligence community would not be doing its job if we did not try to counter that," it says.

A report by **ProPublica and the New York Times** provides some detail about how the agency and GCHQ work together to do this.

Measures are said to include:

- Working with chipmakers to insert backdoors into the code used to carry out encryption, allowing it to be deciphered without the key.
- Maintaining a database of encryption keys for specific commercial products.
- Intercepting a version of the data in its raw form as it is transmitted between a firm's computer servers before being encrypted and sent to the user.
- Carrying out "brute force" attacks - techniques that effectively shorten the length of the key making it easier to guess.

Fallout

Identified **by an alleged NSA slide,** the term appears to refer to an effort to screen out metadata collected about US citizens as part of the Prism programme before it is analysed by the Marina and Mainway systems.

US persons are not supposed to be the subject of the agency's investigations.

Fibre-optic cables

Cables made out of strands of glass as thin as human hair that can transmit data in the form of light across long distances.

Many of these are run along the seabed providing a **variety of routes**for data to criss-cross the globe.

An NSA document published by the **Dutch newspaper NRC Handelsblad** indicates the agency and overseas partner agencies have "20 major accesses" to high-speed optical cables at various points across the globe.

Five Eyes Alliance

The NSA, GCHQ and their counterparts in Canada, Australia and New Zealand.

It is sometimes referred to by the acronym Fvey.

The Nine Eyes Alliance refers to the same group plus Denmark, France, the Netherlands and Norway. The 14 Eyes Alliance adds Belgium, Germany, Italy, Spain and Sweden.

Flatliquid

An operation by the NSA's Tao division that gave the agency access to a mail server used by the Mexican presidential computer network in May 2010, according to **leaks reported by Der Spiegel**.

It said the public email account of Felipe Calderon - who was president at the time - was among those compromised.

Foreign Intelligence Surveillance Act (Fisa)

The original version of this law, passed in 1978, set out the conditions under which a special court would authorise electronic surveillance if people were believed to be engaged in espionage or planning an attack against the US on behalf of a foreign power.

Following the 9/11 attacks, the Bush administration secretly gave the NSA permission to bypass the court and carry out warrantless surveillance of al-Qaeda suspects, among others.

After this emerged in 2005, Congress voted to both offer immunity to the firms that had co-operated with the NSA's requests and to make amendments to Fisa.

The relaxation to the rules, introduced in 2008, meant officials could now obtain court orders without having to identify each individual target or detail the specific types of communications they intended to monitor so long as they convinced the court their purpose was to gather "foreign intelligence information".

In addition, they no longer had to confirm both the sender and receiver of the messages were outside the US, but only had to show it was "reasonable" to believe one of the parties was outside the country.

Foreign Intelligence Surveillance Court (Fisc)

A Washington-based tribunal that considers government agency requests to carry out surveillance for "foreign intelligence purposes" of suspects operating from within the US's borders.

Eleven federal judges make up the panel, each serving a seven-year term. The proceedings are not usually made public.

One of the early Snowden leaks, **published by the Guardian**, documented that the court had granted the FBI permission to collect the telephone metadata records of millions of Verizon customers over a three-month period, rather than just those related to a specific target. The scope of the warrant was **attacked by civil liberty group**s and several politicians as being too broad.

To tackle such concerns, President Obama is **calling on Congress** to establish a panel of "advocates from outside government to provide an independent voice" on significant cases that come before the court.

The president also proposes that the US director of national intelligence and the attorney general hold an annual review to agree which rulings to declassify in order to allow the public to be aware of decisions that have "broad privacy implications".

Foreign Satellite Collection (Fornsat)

A codename that appears **in an alleged NSA presentation** referring to the collection of data from foreign countries' satellites.

A subsequent document, published by the **Dutch newspaper NRC Handelsblad**, indicates that in 2012 the intercept facilities were based in Thailand, Great Britain and Japan, among other countries.

Fouo

An acronym: "for official use only". It appears on several of the leaked documents.

FoxAcid

A tool **reportedly used by the NSA** to study what vulnerabilities a target's computer has. It then uses this knowledge to infect the machine with malware via a web browser.

The agency can subsequently spy on the subject's activity, take control of their equipment or install other exploits.

In some cases this might be an automated process - so the target could be anyone trying to visit a terrorism-themed website. In other cases it might be a specific person identified by their internet address.

Freedom Act

A law proposed by Republican Congressman Jim Sensenbrenner in October 2013 to restrict US agencies' abilities to carry out domestic surveillance.

The full name of the bill is the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act.

Measures include an end to bulk metadata collection and allowing firms to reveal the number of Fisa-related surveillance orders they have complied with.

Genie

An NSA programme, identified in a leaked memo **analysed by the Washington Post**, which is said to involve the remote delivery of spyware to devices on foreign-controlled networks.

The newspaper reports that by the end of 2013, the scheme was expected to control 85,000 implants in machines across the globe. It says the plan was for this data to be analysed by an automated system called Turbine.

Government Communications Headquarters (GCHQ)

The UK government's communications-focussed intelligence agency, employing about 5,000 people.

It dates back to 1919, when it was called the Government Code and Cypher School. It adopted its current name in 1946.

It is based in Cheltenham, Gloucestershire, and also operates two smaller sites in Cornwall and North Yorkshire.

Its two key roles are:

- To identify threats from intercepted communications. It says **these include** terrorism, the spread of nuclear weapons, regional conflicts around the world and threats to the economic prosperity of the UK.
- To serve as an authority on information assurance - meaning that it advises the government and organisations running the UK's critical infrastructure how to safeguard their systems from interference and disruption.

The agency's **website adds**: "Our relationship with the National Security Agency (NSA), the US equivalent of GCHQ, is particularly strong... and remains essential to the security of both nations."

The foreign secretary is answerable in Parliament for GCHQ's work.

G20 summit

One of the early Snowden leaks **involved the Guardian's publication**of alleged GCHQ documents that indicate foreign politicians and officials had their computers and phone calls monitored during two G20 summit meetings hosted in London in 2009.

The report says that the efforts included the creation of internet cafes in which hidden surveillance software had been installed on to PCs; access to messages delivered to Blackberry devices "in near real-time"; and details of who was phoning who at the summit.

Turkey, South Africa and Russia were among nations to **voice concerns**after the publication of the article.

Global Access Operations (GAO)

The branch of the NSA responsible for handling satellite data and other electronic signals.

It was identified as being responsible for the Boundless Informant programme in **leaked documentspublished by the Guardian**.

The leaks indicate that its motto is: "The mission never sleeps."

Greenwald, Glenn

One of three journalists who met Edward Snowden in Hong Kong.

He and another member of the group - Laura Poitras - are **reported to be the only people** known to have access to all the whistleblower's leaked documents.

Mr Greenwald is a former lawyer who initially covered the Snowden leaks for the Guardian.

After a **14-month partnership** he left to set up a new media organisation, although he has subsequently penned an **opinion piece for the paper**.

Mr Greenwald has also written Snowden-related stories for **Huffington Post** and **O Globo**.

Hadoop

An open-source computing platform that lets "big data" computer-based tasks be distributed across thousands of servers and then reassembled when the job is completed.

A report published in 2009 **by InformationWeek** disclosed that the NSA had adopted the system to link up and handle information from the various databases available to it.

The Accumulo data storage and retrieval system it now uses relies on Hadoop to act as its file system.

Hawaii Station

The NSA facility where Edward Snowden worked when he decided to turn whistle-blower.

Its location in the mid-Pacific is near numerous telecoms hubs, making it an ideal location to carry out surveillance of East Asia-based targets.

Hops

A term used to refer to degrees of separation along a chain of contacts.

The NSA used to be allowed to carry out three hops when it identified a suspect. That meant it could look at the phone records of everyone the target spoke to (first hop), everyone this group talked to (second hop), and then all the people they in turn talked to (third hop).

This theoretically meant that the identification of a single target could lead to millions of people's records being investigated. In July 2013 the NSA's deputy director **John Inglis acknowledged** that "a large number" of people could be swept up in a single inquiry. However, he added that this was "not typically what takes place".

In January, President Obama said that he had **ordered the number of hops** to be cut back to two.

Hemlock

A codename used by the NSA for the Italian embassy in Washington, according to leaks **reported by the Guardian**.

It adds that another name used for the same location was Bruneau.

Highlands

The term for data collected from devices bugged with "implants", according to a leaked NSA document **published by Le Monde**.

The paper says this involves pirating information via cookies. However, a later article by Glenn Greenwald **for L'Espresso** suggests it is unclear whether the implants involved are software-based or physical bugs.

Humint

A contraction of "human intelligence" - a phrase used by spy agencies to refer to information gathered from people rather than machines.

Identifiers

A term used by the NSA to refer to information used to recognise a specific individual, This can be their mobile phone number, their log-in details and/or the IP address they are using.

Implants

A term used by spy agencies to refer to software and hardware placed on a target's devices allowing them to access and control them.

Information Need (IN)

The term used for a request to the NSA for details about a foreign entity from another part of the US government or military.

Intelligence and Security Committee of Parliament (ISC)

A panel of nine MPs and Lords responsible for keeping a watch on the policies, administration and expenditure of the UK's security and intelligence agencies, including GCHQ.

To become a member, a politician must first be nominated by the prime minister and then approved by Parliament. After this they gain access to highly classified material.

The committee reports to Parliament and can also send classified reports to the prime minister if the subject is security-sensitive.

The chair of the committee is currently Sir Malcolm Rifkind MP.

Intelligently filtering your data

The title of a leaked NSA presentation, made public by **Brazil's O Globo news network**, that indicated the agency had spied on both Enrique Pena Nieto, in the run-up to his being elected Mexico's president, and Brazil's President Dilma Rousseff as well as her "key advisers".

Intelligence gained is reported to have included text messages from Mr Pena Nieto in which he mentioned the names of advisers he planned to make ministers, and a graph illustrating links between Ms Rousseff's team and other people based on who they had communicated with.

Intelligence Services Act 1994

A **UK law** that defines the boundaries of GCHQ's powers, including details of when its agents require warrants.

Investigatory Powers Tribunal (IPT)

A tribunal, made up of eight senior members of the UK's legal profession, which has the power to investigate complaints about the conduct of GCHQ and the country's other intelligence services and law enforcement agencies.

It has the power to order the organisations to destroy records and provide compensation if it upholds a complaint.

Its current president is Sir Michael Burton.

Joint Apps

An unidentified organisation whose logo featured on a leaked GCHQ document, **published by the Guardian**, that discussed efforts to hack Blackberry devices at a G20 summit.

Some experts have speculated that it might be the successor to the Special Collection Service, a joint CIA/NSA department responsible for covertly planting bugging equipment.

Keyhole

A class of satellites used to send back detailed photographic reconnaissance.

Klondyke

A codename used for an NSA scheme to eavesdrop on the Greek embassy in Washington, according to leaks **reported by the Guardian**.

Laura Poitras

A documentary film-maker and one of three journalists who met Edward Snowden in Hong Kong to receive his stolen defence agency documents.

She and Glenn Greenwald are **reported to be the only people** known to have the full set of leaks.

Lavabit

A "secure email" service that was used by Edward Snowden.

In August 2013 its owner, Ladar Levison, suspended the facility after being ordered to turn over information about one of his accounts. The name of the account's owner is unconfirmed but many **reports assume** it was Snowden's.

Mr Levison refused to hand the data over and also rejected a demand to release the service's encryption keys.

He continues to fight the US government in court and has also joined a group called the **Dark Mail Technical Alliance**, which aims to develop a new encrypted email protocol.

Link Analysis

A tool used by spy agency analysts to identify people linked to a target.

If, for example, they discover the mobile phone number of a suspected terrorist, they could search for it in their metadata records.

If a match is found they could search for everyone that number had called and see for how long the calls lasted and when they occurred.

The contacts of these people could in turn be identified in order to create a chart marking the connections between all the individuals with a probability given of each person being involved in a plot.

MacAskill, Ewen

The Guardian's **defence and intelligence correspondent** - one of three journalists who met Edward Snowden in Hong Kong to receive his leaked defence agency documents.

Mainway

According to the Washington Post's analysis of **NSA leaks**, this is the process used to analyse call record metadata gathered via the Prism programme.

Marina

The NSA's tool to gather metadata about the online activity of targets and other internet users, first detailed in one of the leaked slides about the Prism programme published **by the Washington Post**.

The Guardian later quoted more details **about the scheme** from another NSA document: "The Marina metadata application tracks a user's browser experience, gathers contact information/content and develops summaries of target," it said. "This tool offers the ability to export the data in a variety of formats, as well as create various charts to assist in pattern-of-life development."

According to the leaks, 365 days' worth of such data - including websites visited and map searches, but not the contents of messages - is stored in an associated database.

Marco Civil da Internet

A proposed civil rights law for internet users and providers in Brazil.

Following leaked documents published by **Brazil's Globo television network** - which indicated the NSA had spied on Brazil's President Dilma Rousseff and her Mexican counterpart Enrique Pena Nieto - an amendment was added to the bill.

It said that all internet companies operating in Brazil would have to store copies of personal information about their Brazilian clients in the country. By doing so, the firms providing cloud services would become subject to local privacy laws.

Mastering the Internet (MTI)

A GCHQ initiative, **mentioned in emails seen by the Guardian**, to create an "internet buffer" to let agents review communications that had been sent earlier.

The paper reports the scheme appears to date back to 2007, was first trialled in 2008, and ultimately resulted in the Tempora programme, which was under way by 2011.

Merkel, Angela

In October 2013, Der Spiegel **published a report** suggesting US intelligence agencies had targeted German Chancellor Angela Merkel's mobile phone and had used the American embassy in Berlin as a listening station.

It indicates that a unit called the Special Collection Service - run by both the CIA and NSA - was behind the operation.

The **New York Times later reported** that Mrs Merkel complained about this to President Obama saying: "This is like the Stasi."

The US government has never formally acknowledged the action; however, the **Wall Street Journal reports** that officials told it Mrs Merkel and other world leaders were indeed spied on until a White House review ordered the surveillance to stop.

President Obama has addressed the issue as part of his proposed intelligence-gathering reforms.

"I have made clear to the intelligence community that unless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies," **he said**.

Metadata

Information about a communication rather than details of what was actually said or written - for example, the length of a call, the date of an email, the location a text was sent from, and the type of computer/phone that was used.

According to a **report by the New York Times**, in November 2010 the NSA began allowing its analysts to study large sets of metadata that included records generated by US citizens and others based in the country if they cited a "foreign intelligence justification".

Examples of such a justification include efforts to combat terrorism or an attempt to stop international drug smuggling.

Previously the agents needed to demonstrate they had a "reasonable belief" that the metadata they were studying had been generated by foreigners.

Recently President Obama has **asked the US attorney general** and the intelligence community to draw up plans for metadata to be held by a third party, and proposed that the NSA require legal permission to access it.

Miranda, David

The Brazilian partner of journalist Glenn Greenwald - one of two people known to have full access to the Snowden leaks.

Mr Miranda was detained by UK police for nine hours in August 2013 and had his phone, laptop, memory cards and other items confiscated.

The Home Office argues the police had the right to seize the material, which was believed to include copies of some of the leaked documents.

However, Mr Miranda's lawyers say the Terrorism Act 2000 used to justify the confiscations does not apply to such "journalistic material".

Muscular

A joint project operated by the NSA and GCHQ as part of the American agency's Windstop programme.

Leaked documents indicate it has been used to intercept data from the cable links that are used by **Google** and others to connect up their computer servers, which are located across the world .

According to a slide published by the Washington Post, GCHQ began collecting data as part of the Muscular programme in July 2009.

At the time it could hold up to **10 gigabytes of processed traffic a day**- but the paper says that was scheduled to have risen by four times by now.

National Security Agency (NSA)

The US government agency tasked with gathering intelligence for the country's government and military leaders, and preventing foreign adversaries from gaining access to classified national security information.

The NSA employs about 35,000 workers, both civilians and military, and its budget for 2013 was $10.8bn (£6.7bn). However, a **report by the Financial Times noted** that once spending on the management of the satellites it uses and other related military services' operations were taken into account, the sum more than doubled.

National Security Letter

Requests, authorised by the FBI, that compel US companies to hand over "the name, address, length of service" and other records linked to one or more of their subscribers as part of a national security investigation.

National Cyber Security Strategy

A document, **published in November 2011**, detailing how the UK intended to tackle internet-based threats.

Among its objectives is the goal of enhancing the "world-class technical skills" of GCHQ's staff.

Noforn

A term used by the US government to mean "no foreign nationals" - indicating a document should not be shared with non-US citizens.

Nucleon

An NSA **slide indicates** that this is the process used to analyse voice data gathered via the Prism programme.

Offensive Cyber Effects Operations (Oceo)

An alleged 2012 classified presidential memo, **published by the Guardian**, discusses drawing up a list of of overseas targets that could potentially by examined by Oceo.

Oceo is defined as programmes or activities involving "unique and unconventional capabilities" that can be carried out via cyberspace.

Office of the Director of National Intelligence (ODNI)

The head of the US intelligence community, in charge of 17 organisations and agencies including the NSA, FBI and CIA.

James Clapper has held the position since 2010.

Organization of the Petroleum Exporting Countries (Opec)

The Vienna-based oil cartel created in the 1960s to influence energy prices by co-ordinating production. It **currently has 12 members**including Saudi Arabia, Venezuela and Iran.

Snowden leaks **reported by Der Spiegel** indicate both the NSA and GCHQ have infiltrated Opec's computer network.

The article notes that as of April 2013, the US no longer listed the organisation as a "high-priority target" because the country was less dependent on its petroleum.

Perdido

The codename for an NSA surveillance operation targeting the EU's offices in New York and Washington, according to leaked documents**seen by the Guardian**.

Powell

A codename used for an NSA scheme to eavesdrop on the Greek United Nation offices in New York, according to leaked documents **reported by the Guardian**.

Public Breach Exchange Switch (PBX)

A term referenced by a leaked NSA document **published by Le Monde**.

It has been speculated that it refers to a system that exploits vulnerabilities in "private branch exchange switches" - a system used by businesses to share telephone lines to avoid having to pay for a separate one for each worker's handset.

Le Monde reports that PBX has been used to eavesdrop on conversations between French diplomats.

Pinwale

Identified **by an NSA slide,** the codename appears to refer to a database used to store and analyse video and other selected content gathered by Prism and other programmes.

Prefer

An NSA system, identified by **leaked papers published** by the Guardian, that extracts information from SMS text data gathered by the Dishfire programme.

The newspaper **says this involves** scanning automated messages - such as missed call alerts and international roaming charge texts sent when a handset crosses a border - to increase the range of metadata gathered.

Printaura

An automated system used by the NSA, which reportedly **takes the data collected via Prism** and then identifies and sorts it into at least 11 different categories, including log-ins, photos, videos and metadata.

Prism

A surveillance system launched in 2007 by the NSA.

A **leaked presentation**, dated April 2013, states that it allows the organisation to "receive" emails, video clips, photos, voice and video calls, social networking details, log-ins and other data held by a range of US internet firms.

The slides identify seven companies as being providers to the programme: Apple, AOL, Facebook, Google (including YouTube), Microsoft (including Skype), Paltalk and Yahoo.

According to documents **published by the Washington Post**, the NSA obtained at least some of the information via the FBI, which has placed "government equipment" on the private property of participating companies.

The newspaper adds that as a result, the NSA has access to real-time surveillance, including notifications showing when a target logged on or sent an email, as well as the ability to monitor voice and text chats as they happen.

However, Apple's chief executive Tim Cook has been among tech firm leaders to stress that the US **government has "no back door"** into company servers.

The Guardian reports that GCHQ has been **carrying out its own analysis** of Prism-gathered data since at least 2010.

Protect America Act (PAA) 2007

A law designed to address a surveillance gap caused by a classified court ruling,

The Washington Post reports that **the ruling said** it was illegal to intercept a communication that began and ended abroad if any of the data passed through the US.

PAA made it possible for such surveillance to be carried out if officials said "reasonable procedures" existed to ensure their target was located outside the US.

The paper suggests this "vague requirements" allowed the Prism scheme to be launched.

QuantumInsert

A "man-in-the-middle" technique used to redirect a target's computer to a fake website where it can be infected with malware.

The NSA and GCHQ are **said to do this** by placing undisclosed computer servers at privileged positions along the fibre-optic cables that form the internet's backbone.

These servers provide the agencies with the ability to reply to a web page request more quickly than the computers used by the site the user is trying to visit.

The agencies are alleged to do this in order to route the user to a spoof site. This looks identical to the real one but exists solely to install spyware using the NSA's FoxAcid tool.

According to a **report by Der Spiegel,** the QuantumInsert system was used by GCHQ to infiltrate Brussels-based telecoms operator Belgacom's systems by using fake pages for the LinkedIn social network and the tech news site Slashdot - two sites commonly visited by several of the firm's maintenance and security staff.

Rampart-T

An NSA operation, **according to leaks reported by Der Spiegel**, that targeted the communications of heads of states and their aides.

It said the scheme dates back to at least 1991 and was directed against 20 countries including Russia, China and Eastern European countries.

Real Time Regional Gateway (RTRG)

A data-collection and management system that the NSA **first deployed in Iraq** and then later Afghanistan.

It took data including military events, phone conversations, opinion polls and the price of goods to predict where and when violence would occur.

The success of the effort is **reported to have influenced** NSA director Keith Alexander's desire for the agency's other data-collecting efforts to have access to a multitude of sources

Reasonable belief

US law prevents the NSA from targeting any US citizen, any other US person, or anyone located within the United States.

However, a relaxation to the **country's surveillance rules in 2008**meant that the agency no longer had to confirm both the sender and receiver of a message were outside the country. Instead the agency only had to demonstrate it "reasonably believed" this to be the case.

According to the Washington Post, this has been interpreted to mean that checks carried out as part of the Prism programme only need to deliver a "51% confidence" rating that a target is foreign. It has not been disclosed how this score is calculated.

Regulation of Investigatory Powers Act 2000

A UK law **used to authorise** the covert interception of communications by public bodies.

It made it a criminal offence to refuse an order to hand over encryption keys.

Remote Operations Centre (Roc)

The name given to the headquarters of the NSA's Tao group of hackers, according to officials who spoke to the **Foreign Policy journal**.

Renoir

A program **used by the NSA** to view graphical representations of the data it holds.

Royal Concierge

A computer system used by GCHQ to track foreign diplomats' hotel reservations, according to a leaked paper **published by Der Spiegel**.

The magazine reports that it has been in use since at least 2010 and allows the agency to monitor bookings in at least 350 upmarket hotels around the world.

Once the hotel room is identified, it says, a team codenamed Teca can be deployed to monitor the target's communications.

The scheme appears to have its own logo: a penguin wearing a crown and holding a wand.

RSA

In September 2013 the **New York Times published** an article alleging that the US government had coerced some companies into building a "back door" into their encryption products.

In December, **Reuters reported** that one of the compromised tools was BSafe - software offered by security firm RSA, a division of IT giant EMC.

The article alleges that one of the product's default random number generators had been compromised and that RSA had been paid $10m (£6m) to set it as the default option.

RSA **says it categorically denies** entering into a "secret contract" to incorporate a "known flawed random number generator".

However, several security experts who had been due to speak at the firm's annual US conference in February have cancelled their presentations and are now planning to attend an alternative event in the same city **dubbed Trustycon**.

Selectors

The identifiers used by the security services when carrying out their searches - for example, a phone number or an internet protocol (IP) address. These can be divided into two broad types - strong and soft.

A strong selector is an identifier associated with a specific individual - eg a search for content associated with an email address. In theory, the NSA cannot intentionally use a strong selector linked to a US citizen, any other US person or anyone located within the United States.

A soft selector is less limited in its scope and is typically based on the content of message. This can be a word or phrase, such as "big explosion", or the language the message is written in - for example, French.

Serendipity

Tools that were apparently developed by the NSA to handle data captured from Google's internal network as part of the Muscular programme. The agency needed to do this because Google used a proprietary data format when transferring files between its servers.

According to a slide published by the Washington Post, the agency was able to distinguish the information by type, eg data from the search firm's Picasa photo service, its YouTube video platform and its Chrome sync service, which copies browser settings and bookmarks from one computer to another.

Two **of Google'sengineers reacted** with fury to the news. They noted that the firm had now begun encrypting the data referred to in the slides, and that as a consequence the NSA and GCHQ's efforts to understand it were "ruined".

Session

A term for a data exchange between two computers. This can be prompted by a user entering log-in details for an online service or the transfer of a chat message.

Sigint

An abbreviation of "signals intelligence", the term used for the gathering of information from electronic signals and systems, whether created by humans or machines.

This can include the monitoring of internet communications, the use of radars, weapons systems or other equipment.

Signals Intelligence Activity Designator (Sigad)

The NSA gives a Sigad code to each of its sources of intelligence.

For example the Sigad name for the Prism programme is reported to be US-984XN.

Social Network Analysis Collaboration Knowledge Services (Snacks)

An NSA programme, **identified by the New York Times**, that analyses text messages to deduce the personnel hierarchies of targeted organisations.

Snowden, Edward
A former CIA technician who is the source of leaked documents that appear to detail the activities of the NSA, GCHQ and other intelligence agencies.

Snowden left the CIA in 2009 and joined Dell, **where Reuters reports**he first began downloading material on the governments' eavesdropping efforts.

He then moved to another security contractor, Booz Allen Hamilton, who placed him at an NSA regional centre in Hawaii.

Snowden later **told the South China Morning Post** he had taken this job in order to gather material about machines the NSA had hacked into.

After three months he quit and moved to Hong Kong where he shared the material with journalists.

He is currently living in Russia, where he has been granted temporary asylum, but Snowden says he ultimately **wishes to return to the US**.

However, the US Justice Department has charged him with violations of the Espionage Act and President Obama has said he should stand trial.

Socialist

The name given to a GCHQ operation to hack into the systems of the Belgian telecoms provider Belgacom, according to Snowden leaks reported by **Der Spiegel**.

The magazine's initial report said the papers indicated the British spy agency had used NSA-developed technologies to achieve its goal.

A **follow-up article** later added that fake web pages that pretended to belong to the social network LinkedIn and the news site Slashdot had been used to infect computers of Belgacom employees who visited the sites.

Special Collection Service (SCS)

According to Der Spiegel, a **2010 NSA leaked document** revealed that agents belonging to a unit known as the SCS were active in 80 locations around the world.

It said the organisation was an "elite corps" run by both the NSA and CIA that monitored cellular signals, wireless networks and satellite communications via equipment fitted to US embassy buildings.

The magazine suggested one of these entities had been involved in targeting a mobile phone used by German Chancellor Angela Merkel.

Special Source Operations (SSO)

A division of the NSA responsible for overseeing programmes that source their data through "partnerships" with US and overseas-based companies.

This includes data demanded from cloud service providers as part of Prism, and companies which provide the fibre-optic cables and routers that form the backbone of the internet.

Squeaky Dolphin

A GCHQ operation that analysed YouTube video views, Facebook "likes" and Blogger visits gathered from tapped optic-fibre cables, according to a leaked presentation **published by NBC News**.

It said the UK agency showed off its abilities to US counterparts at the NSA, in 2012.

Examples that GCHQ is said to have demonstrated include:

- a table showing how many people based in the city of Lagos looked at a specific job vacancies blog over a 24-hour period
- a graph showing how many London-based internet users "liked" links about former defence secretary Liam Fox on Facebook over a week-long period
- a pie chart highlighting 20 tending YouTube video tags a day before planned anti-government protests in Bahrain

Although the examples provided did not identify specific users, **NBC suggested** this would have been possible to do if GCHQ had access to such data.

Stellarwind

A metadata-collecting scheme dated back to 2001, which was first identified by the **New York Times and Newsweek** seven years later.

It was initially limited to collecting metadata from communications in which at least one party was outside the US, and none of the other parties could be known to be US citizens. This restriction was later relaxed.

The scheme originally operated without the oversight of a judge, but after briefly being halted, came under the authority of the Fisa court in 2004.

The **Guardian reported** that the effort was eventually brought to an end during President Obama's first administration.

Tailored Access Operations (Tao)

A division of the NSA, which the agency says is "centred on computer network exploitation".

Leaked documents **reported by Der Spiegel** describe the unit's job as "getting the ungettable".

The magazine likened it to a squad of "digital plumbers" - hackers capable of gaining access to data thought to be secure.

It has reported that operations carried out by the unit include:

- Surveillance of **Mexican government networks** including access to ex-President Felipe Calderon's public email account.
- Taking advantage of error reports sent by Microsoft Windows to identify potential security holes in targets' computers.
- Hacking the internal website of the operator of an underwater cable system connecting Europe, North Africa and parts of Asia, revealing details about its technical infrastructure.
- Gaining physical access to targets, including networks not connected to the internet.

Tempora

The codename given to an operation to create a "buffer" to allow huge amounts of data to be temporarily stored for analysis.

According to **documents reported by The Guardian**, the scheme is run by GCHQ and began at the end of 2011. It says the agency holds content gathered from tapped fibre-optic cables for three days and metadata for 30 days so that both it and the NSA can search and analyse it before details are lost.

The newspaper adds that in 2012 the British spy agency had tapped more than 200 cables - including transatlantic communication links - and was able to process phone and internet data taken from up to 46 of them at a time.

Thinthread

A proposed NSA system to chart relationships between people in real-time.

Details of the project were published **by the New Yorker magazine**which interviewed one of its architects, Bill Binney, in 2011.

Mr Binney said the plan had been to correlate data from "financial transactions, travel records, web searches, GPS equipment, and any other 'attributes'" that might help identify "bad guys". Rather than send the data back to the NSA's headquarters for analysis, the system was designed to process information as it was collected and only retain the important details.

Pilot tests were carried out at the turn of the millennium. Mr Binney said they threw up a problem: large amounts of data were being picked up about US persons, which the NSA was not allowed to collect. He said he added a feature to encrypt such communications so that they could not be read by unless a warrant was issued to permit them to be decoded.

However, it is reported that the NSA opted instead for a more ambitious and expensive alternative - codenamed Trailblazer - which later ran into problems of its own.

Tippers

The name used by the NSA **for alert messages** and other early-stage reports used to highlight anticipated or actual events to relevant officials.

Tor

Invented by the US Naval Research Laboratory to help people use the web without being traced, Tor (The Onion Router) aids anonymity in two ways.

First, it can be used to browse the world wide web anonymously. It does this by routing traffic through many separate encrypted layers to hide the data identifiers that prove useful in police investigations.

Second, there are hidden sites on Tor that use the .onion domain suffix. These are effectively websites but, as they sit on Tor, are almost impervious to investigation.

Journalists and whistle-blowers use Tor to communicate with each other, but an alleged NSA presentation, **published by the Guardian**, highlights that terrorists and other surveillance targets also use it.

Another **Snowden leak states** "Tor stinks", adding that the NSA will never be able to de-anonymise all its users all of the time.

However, operations including EgotisticalGiraffe indicate the agency has found ways to track some people using the service.

Tracfin

A database of financial transactions collected by the NSA, according to leaked documents **reported by Der Spiegel**.

It says these include international payments, credit card purchases and banking transactions.

The report adds that the documents suggest one of the sources for the agency's information was the Society for Worldwide Interbank Financial Transactions (Swift) - a network used by thousands of lenders to share information securely.

Trailblazer

The name given to a programme commissioned in about 2000 to overhaul how the NSA sifted and analysed phone and internet data.

Many of the details about it were made public in a series of articles published by the **Baltimore Sun newspaper**. It said the project was supposed to have been built by outside contractors.

However, it was cancelled in 2006 **after an estimated $1.2bn** (£720m) had been spent on the scheme when it became clear it was struggling to achieve its goals.

Its failure led to the creation of another project, Turbulence.

Turbulence

An NSA initiative to identify potential threats by scanning internet traffic.

The Baltimore Sun published the first reports about it in 2007.

The newspaper said that at the time the project had nine core programmes whose names also began with the letter T.

Turbulence was later referenced in a leaked training materials for XKeyscore, **published by the Guardian**.

Slides **published by Der Spiegel** subsequently contained further detail, indicating that Turbulence's programmes include:

- Tumult: the demultiplexing of captured signals. This involves extracting the various data streams that have been combined so that they can be analysed.
- Turmoil: deep packet inspection of data gathered from foreign target satellites, fibre cables and microwave-based communications.
- Turbine: deep packet injection - a technique used to place automated "command and control" implants on targets' machines, effectively creating a government-controlled botnet.
- Tutelage: detecting incoming cyber-attacks to allow the NSA to block them or manipulate the code to its own advantage.

Upstream programme

Identified by **an NSA document** as the "collection of communications on fibre cables and infrastructure as data flows past".

Senate Intelligence Committee Chair Dianne Feinstein **appeared to confirm the practice** in September when she read a statement saying: "Upstream collection… occurs when NSA obtains internet communications, such as emails, from certain US companies that operate the internet background [likely a reference to the internet backbone], ie the companies that own and operate the domestic telecommunication lines over which internet traffic flows."

The implication is that the agency is able to obtain and study communications without having to request the information from internet companies, using its Prism programme.

The name of four such operations were identified as: Blarney, Fairview, Oakstar and Stormbrew.

Vagrant

The term for data collected from bugged computer screens, according to a leaked NSA document **published by Le Monde**.

Verizon

The first of the Snowden leaks to be made public suggested **the FBI was collecting metadata** about calls made by millions of customers of the US network Verizon.

It said the information was then passed to the NSA for analysis.

US judges have issued contradictory rulings as to whether or not the bulk collection and storage of so much information is legal under the Patriot Act.

President Obama has called on the intelligence agencies to **suggest an alternative approach** that would not require the NSA to hold the metadata itself. However, he noted that giving the job to a third party could entail extra expense and potentially end up being less accountable.

Wabush

An NSA operation that targeted data held by French diplomats in the country's Washington embassy, according to a **paper seen by Der Spiegel**.

Whitetamale

Snowden leaks **reported by Der Spiegel** describe an operation carried out in Mexico that gave the NSA access to emails of officials in the country's Public Security Secretariat.

The agency was responsible for preserving order, and its tasks included tackling the drugs trade.

Windstop

NSA data-collection programmes that depend on help from Britain, Canada, Australia and New Zealand.

A document **published by the Washington Post suggests** that the programmes accounted for 181 million records being sent to the agency from a British collection point over a 30-day period towards the end of 2012.

XKeyscore

According to NSA training documents **quoted by the Guardian** this is the agency's "widest-reaching" system for internet surveillance covering "nearly everything a typical user does" online.

It says analysts can search by selecting the user's name, their IP address, keywords in the contents of their communications - including emails and Facebook posts - or by selecting certain metadata criteria.

Due to the large amount of data being gathered, the paper reports that content is stored for between one to five days, and metadata up to a month. However, it adds, "interesting" material can be stored in one of the NSA's other databases.

The NSA issued a statement to the paper saying that every search was "fully auditable, to ensure they are proper and within the law".