

# National Security Agency

The **National Security Agency** (**NSA**) is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence. The NSA is responsible for global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT). The NSA is also tasked with the protection of U.S. communications networks and information systems.<sup>[8][9]</sup> The NSA relies on a variety of measures to accomplish its mission, the majority of which are clandestine.<sup>[10]</sup>

Originating as a unit to decipher coded communications in World War II, it was officially formed as the NSA by President Harry S. Truman in 1952. Since then, it has become the largest of the U.S. intelligence organizations in terms of personnel and budget.<sup>[6][11]</sup> The NSA currently conducts worldwide mass data collection and has been known to physically bug electronic systems as one method to this end.<sup>[12]</sup> The NSA is also alleged to have been behind such attack software as Stuxnet, which severely damaged Iran's nuclear program.<sup>[13][14]</sup> The NSA, alongside the Central Intelligence Agency (CIA), maintains a physical presence in many countries across the globe; the CIA/NSA joint Special Collection Service (a highly classified intelligence team) inserts eavesdropping devices in high value targets (such as presidential palaces or embassies). SCS collection tactics allegedly encompass "close surveillance, burglary, wiretapping, [and] breaking and entering".<sup>[15][16]</sup>

Unlike the CIA and the Defense Intelligence Agency (DIA), both of which specialize primarily in foreign human espionage, the NSA does not publicly conduct human-source intelligence gathering. The NSA is entrusted with providing assistance to, and the coordination of, SIGINT elements for other government organizations – which are prevented by law from engaging in such activities on their own.<sup>[17]</sup> As part of these responsibilities, the agency has a co-located organization called the Central Security Service

## National Security Agency



Seal of the National Security Agency



Flag of the National Security Agency



NSA Headquarters, Fort Meade, Maryland

### Agency overview

<b>Formed</b>	November 4, 1952 <sup>[1]</sup>
<b>Preceding agency</b>	Armed Forces Security Agency
<b>Headquarters</b>	<u>Fort Meade, Maryland, U.S.</u> <u><span><span><span><span><span>39°6′32″N</span> <span>76°46′17″W</span></span></span><span><span>﻿</span> / <span>﻿</span></span><span><span></span></span></span></span></u>
<b>Motto</b>	"Defending Our Nation. Securing the Future."
<b>Employees</b>	Classified (est. 30,000–40,000) <sup>[2][3][4][5]</sup>
<b>Annual budget</b>	Classified (estimated \$10.8 billion, 2013) <sup>[6][7]</sup>
<b>Agency executives</b>	<u>General Paul M. Nakasone, U.S. Army, Director</u> <u>George C. Barnes, Deputy Director</u>

(CSS), which facilitates cooperation between the NSA and other U.S. defense cryptanalysis components. To further ensure streamlined communication between the signals intelligence community divisions, the NSA Director simultaneously serves as the Commander of the United States Cyber Command and as Chief of the Central Security Service.

<b>Parent agency</b>	<u>Department of Defense</u>
<b>Website</b>	<u>NSA.gov (https://www.nsa.gov)</u>

The NSA's actions have been a matter of political controversy on several occasions, including its spying on anti-Vietnam War leaders and the agency's participation in economic espionage. In 2013, the NSA had many of its secret surveillance programs revealed to the public by Edward Snowden, a former NSA contractor. According to the leaked documents, the NSA intercepts and stores the communications of over a billion people worldwide, including United States citizens. The documents also revealed the NSA tracks hundreds of millions of people's movements using cellphones' metadata. Internationally, research has pointed to the NSA's ability to surveil the domestic Internet traffic of foreign countries through "boomerang routing".<sup>[18]</sup>

## Contents

---

### History

- Formation
- The Black Chamber
- World War II and its aftermath
- Vietnam War
- Church Committee hearings
- From 1980s to 1990s
- War on Terror
- Global surveillance disclosures

### Mission

### Operations

- Collection overseas
  - Echelon
  - Other SIGINT operations overseas
  - Boundless Informant
  - Bypassing encryption
  - Software backdoors
  - Boomerang routing
  - Hardware implanting
- Domestic collection
  - President's Surveillance Program
  - The PRISM program
- Hacking operations

### Organizational structure

- Directorates
- NSANet
- Watch centers
- Employees

[Personnel security](#)

[Polygraphing](#)

[Arbitrary firing](#)

## **[Facilities](#)**

[Headquarters](#)

[History of headquarters](#)

[Power consumption](#)

[Computing assets](#)

[National Computer Security Center](#)

[Other U.S. facilities](#)

[International stations](#)

[Thailand](#)

## **[Research and development](#)**

[Data Encryption Standard](#)

[Advanced Encryption Standard](#)

[NSA encryption systems](#)

[SHA](#)

[Clipper chip](#)

[Dual\\_EC\\_DRBG random number generator cryptotrojan](#)

[Perfect Citizen](#)

[Academic research](#)

[Patents](#)

## **[Insignia and memorials](#)**

## **[Controversy and litigation](#)**

[Warrantless wiretaps](#)

[AT&T Internet monitoring](#)

[Data mining](#)

[Illegally obtained evidence](#)

[Barack Obama administration](#)

[Section 215 metadata collection](#)

[Fourth Amendment encroachment](#)

[Congressional oversight](#)

[Official responses](#)

[Responsibility for international ransomware attack](#)

[2015 Michelle Obama email hack](#)

## **[See also](#)**

## **[Notes](#)**

## **[References](#)**

## **[Further reading](#)**

## **[External links](#)**

# **History**

---

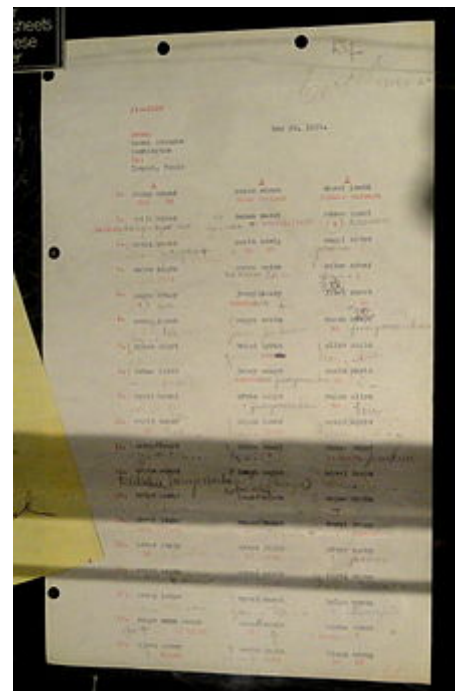
## Formation

The origins of the National Security Agency can be traced back to April 28, 1917, three weeks after the U.S. Congress declared war on Germany in World War I. A code and cipher decryption unit was established as the Cable and Telegraph Section which was also known as the Cipher Bureau.<sup>[19]</sup> It was headquartered in Washington, D.C. and was part of the war effort under the executive branch without direct Congressional authorization. During the course of the war, it was relocated in the army's organizational chart several times. On July 5, 1917, Herbert O. Yardley was assigned to head the unit. At that point, the unit consisted of Yardley and two civilian clerks. It absorbed the Navy's cryptanalysis functions in July 1918. World War I ended on November 11, 1918, and the army cryptographic section of Military Intelligence (MI-8) moved to New York City on May 20, 1919, where it continued intelligence activities as the Code Compilation Company under the direction of Yardley.<sup>[20][21]</sup>

## The Black Chamber

After the disbandment of the U.S. Army cryptographic section of military intelligence, known as MI-8, in 1919, the U.S. government created the Cipher Bureau, also known as Black Chamber. The Black Chamber was the United States' first peacetime cryptanalytic organization.<sup>[22]</sup> Jointly funded by the Army and the State Department, the Cipher Bureau was disguised as a New York City commercial code company; it actually produced and sold such codes for business use. Its true mission, however, was to break the communications (chiefly diplomatic) of other nations. Its most notable known success was at the Washington Naval Conference, during which it aided American negotiators considerably by providing them with the decrypted traffic of many of the conference delegations, most notably the Japanese. The Black Chamber successfully persuaded Western Union, the largest U.S. telegram company at the time, as well as several other communications companies to illegally give the Black Chamber access to cable traffic of foreign embassies and consulates.<sup>[23]</sup> Soon, these companies publicly discontinued their collaboration.

Despite the Chamber's initial successes, it was shut down in 1929 by U.S. Secretary of State Henry L. Stimson, who defended his decision by stating, "Gentlemen do not read each other's mail."<sup>[24]</sup>



Black Chamber cryptanalytic work sheet for solving Japanese diplomatic cipher, 1919

## World War II and its aftermath

During World War II, the Signal Intelligence Service (SIS) was created to intercept and decipher the communications of the Axis powers.<sup>[25]</sup> When the war ended, the SIS was reorganized as the Army Security Agency (ASA), and it was placed under the leadership of the Director of Military Intelligence.<sup>[25]</sup>

On May 20, 1949, all cryptologic activities were centralized under a national organization called the Armed Forces Security Agency (AFSA).<sup>[25]</sup> This organization was originally established within the U.S. Department of Defense under the command of the Joint Chiefs of Staff.<sup>[26]</sup> The AFSA was tasked to direct Department of Defense communications and electronic intelligence activities, except those of U.S. military intelligence units.<sup>[26]</sup> However, the AFSA was unable to centralize communications intelligence and failed to coordinate with civilian agencies that shared its interests such as the Department of State, Central Intelligence Agency

(CIA) and the Federal Bureau of Investigation (FBI).<sup>[26]</sup> In December 1951, President Harry S. Truman ordered a panel to investigate how AFSA had failed to achieve its goals. The results of the investigation led to improvements and its redesignation as the National Security Agency.<sup>[27]</sup>

The National Security Council issued a memorandum of October 24, 1952, that revised National Security Council Intelligence Directive (NSCID) 9. On the same day, Truman issued a second memorandum that called for the establishment of the NSA.<sup>[28]</sup> The actual establishment of the NSA was done by a November 4 memo by Robert A. Lovett, the Secretary of Defense, changing the name of the AFSA to the NSA, and making the new agency responsible for all communications intelligence.<sup>[29]</sup> Since President Truman's memo was a classified document,<sup>[28]</sup> the existence of the NSA was not known to the public at that time. Due to its ultra-secrecy the U.S. intelligence community referred to the NSA as "No Such Agency".<sup>[30]</sup>

## Vietnam War

In the 1960s, the NSA played a key role in expanding U.S. commitment to the Vietnam War by providing evidence of a North Vietnamese attack on the American destroyer USS Maddox during the Gulf of Tonkin incident.<sup>[31]</sup>

A secret operation, code-named "MINARET", was set up by the NSA to monitor the phone communications of Senators Frank Church and Howard Baker, as well as key leaders of the civil rights movement, including Martin Luther King Jr., and prominent U.S. journalists and athletes who criticized the Vietnam War.<sup>[32]</sup> However, the project turned out to be controversial, and an internal review by the NSA concluded that its Minaret program was "disreputable if not outright illegal".<sup>[32]</sup>

The NSA mounted a major effort to secure tactical communications among U.S. forces during the war with mixed success. The NESTOR family of compatible secure voice systems it developed was widely deployed during the Vietnam War, with about 30,000 NESTOR sets produced. However, a variety of technical and operational problems limited their use, allowing the North Vietnamese to exploit and intercept U.S. communications.<sup>[33]</sup> :Vol I, p.79

## Church Committee hearings

In the aftermath of the Watergate scandal, a congressional hearing in 1975 led by Senator Frank Church<sup>[34]</sup> revealed that the NSA, in collaboration with Britain's SIGINT intelligence agency Government Communications Headquarters (GCHQ), had routinely intercepted the international communications of prominent anti-Vietnam war leaders such as Jane Fonda and Dr. Benjamin Spock.<sup>[35]</sup> The Agency tracked these individuals in a secret filing system that was destroyed in 1974.<sup>[36]</sup> Following the resignation of President Richard Nixon, there were several investigations of suspected misuse of FBI, CIA and NSA facilities.<sup>[37]</sup> Senator Frank Church uncovered previously unknown activity,<sup>[37]</sup> such as a CIA plot (ordered by the administration of President John F. Kennedy) to assassinate Fidel Castro.<sup>[38]</sup> The investigation also uncovered NSA's wiretaps on targeted U.S. citizens.<sup>[39]</sup>

After the Church Committee hearings, the Foreign Intelligence Surveillance Act of 1978 was passed. This was designed to limit the practice of mass surveillance in the United States.<sup>[37]</sup>

## From 1980s to 1990s

In 1986, the NSA intercepted the communications of the Libyan government during the immediate aftermath of the Berlin discotheque bombing. The White House asserted that the NSA interception had provided "irrefutable" evidence that Libya was behind the bombing, which U.S. President Ronald Reagan cited as a

justification for the 1986 United States bombing of Libya.<sup>[40][41]</sup>

In 1999, a multi-year investigation by the European Parliament highlighted the NSA's role in economic espionage in a report entitled 'Development of Surveillance Technology and Risk of Abuse of Economic Information'.<sup>[42]</sup> That year, the NSA founded the NSA Hall of Honor, a memorial at the National Cryptologic Museum in Fort Meade, Maryland.<sup>[43]</sup> The memorial is a, "tribute to the pioneers and heroes who have made significant and long-lasting contributions to American cryptology".<sup>[43]</sup> NSA employees must be retired for more than fifteen years to qualify for the memorial.<sup>[43]</sup>

NSA's infrastructure deteriorated in the 1990s as defense budget cuts resulted in maintenance deferrals. On January 24, 2000, NSA headquarters suffered a total network outage for three days caused by an overloaded network. Incoming traffic was successfully stored on agency servers, but it could not be directed and processed. The agency carried out emergency repairs at a cost of \$3 million to get the system running again. (Some incoming traffic was also directed instead to Britain's GCHQ for the time being.) Director Michael Hayden called the outage a "wake-up call" for the need to invest in the agency's infrastructure.<sup>[44]</sup>

In the 1990s the defensive arm of the NSA—the Information Assurance Directorate (IAD)—started working more openly; the first public technical talk by an NSA scientist at a major cryptography conference was J. Solinas' presentation on efficient Elliptic Curve Cryptography algorithms at Crypto 1997.<sup>[45]</sup> The IAD's cooperative approach to academia and industry culminated in its support for a transparent process for replacing the outdated Data Encryption Standard (DES) by an Advanced Encryption Standard (AES). Cybersecurity policy expert Susan Landau attributes the NSA's harmonious collaboration with industry and academia in the selection of the AES in 2000—and the Agency's support for the choice of a strong encryption algorithm designed by Europeans rather than by Americans—to Brian Snow, who was the Technical Director of IAD and represented the NSA as cochairman of the Technical Working Group for the AES competition, and Michael Jacobs, who headed IAD at the time.<sup>[46]:75</sup>

After the terrorist attacks of September 11, 2001, the NSA believed that it had public support for a dramatic expansion of its surveillance activities.<sup>[47]</sup> According to Neal Koblitz and Alfred Menezes, the period when the NSA was a trusted partner with academia and industry in the development of cryptographic standards started to come to an end when, as part of the change in the NSA in the post-September 11 era, Snow was replaced as Technical Director, Jacobs retired, and IAD could no longer effectively oppose proposed actions by the offensive arm of the NSA.<sup>[48]</sup>

## War on Terror

In the aftermath of the September 11 attacks, the NSA created new IT systems to deal with the flood of information from new technologies like the Internet and cellphones. ThinThread contained advanced data mining capabilities. It also had a "privacy mechanism"; surveillance was stored encrypted; decryption required a warrant. The research done under this program may have contributed to the technology used in later systems. ThinThread was cancelled when Michael Hayden chose Trailblazer, which did not include ThinThread's privacy system.<sup>[49]</sup>

Trailblazer Project ramped up in 2002 and was worked on by Science Applications International Corporation (SAIC), Boeing, Computer Sciences Corporation, IBM, and Litton Industries. Some NSA whistleblowers complained internally about major problems surrounding Trailblazer. This led to investigations by Congress and the NSA and DoD Inspectors General. The project was cancelled in early 2004.

Turbulence started in 2005. It was developed in small, inexpensive "test" pieces, rather than one grand plan like Trailblazer. It also included offensive cyber-warfare capabilities, like injecting malware into remote computers. Congress criticized Turbulence in 2007 for having similar bureaucratic problems as Trailblazer.<sup>[50]</sup> It was to be a realization of information processing at higher speeds in cyberspace.<sup>[51]</sup>

## Global surveillance disclosures

The massive extent of the NSA's spying, both foreign and domestic, was revealed to the public in a series of detailed disclosures of internal NSA documents beginning in June 2013. Most of the disclosures were leaked by former NSA contractor Edward Snowden. On 4 September 2020, the NSA's surveillance program was ruled unlawful by the US Court of Appeals. The court also added that the US intelligence leaders, who publicly defended it, were not telling the truth.<sup>[52]</sup>

## Mission

---

NSA's eavesdropping mission includes radio broadcasting, both from various organizations and individuals, the Internet, telephone calls, and other intercepted forms of communication. Its secure communications mission includes military, diplomatic, and all other sensitive, confidential or secret government communications.<sup>[53]</sup>

According to a 2010 article in *The Washington Post*, "[e]very day, collection systems at the National Security Agency intercept and store 1.7 billion e-mails, phone calls and other types of communications. The NSA sorts a fraction of those into 70 separate databases."<sup>[54]</sup>

Because of its listening task, NSA/CSS has been heavily involved in cryptanalytic research, continuing the work of predecessor agencies which had broken many World War II codes and ciphers (see, for instance, Purple, Venona project, and JN-25).

In 2004, NSA Central Security Service and the National Cyber Security Division of the Department of Homeland Security (DHS) agreed to expand the NSA Centers of Academic Excellence in Information Assurance Education Program.<sup>[55]</sup>

As part of the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD 54), signed on January 8, 2008, by President Bush, the NSA became the lead agency to monitor and protect all of the federal government's computer networks from cyber-terrorism.<sup>[9]</sup>

## Operations

---

Operations by the National Security Agency can be divided into three types:

- Collection overseas, which falls under the responsibility of the Global Access Operations (GAO) division.
- Domestic collection, which falls under the responsibility of the Special Source Operations (SSO) division.
- Hacking operations, which fall under the responsibility of the Tailored Access Operations (TAO) division.

## Collection overseas

### Echelon

"Echelon" was created in the incubator of the Cold War.<sup>[56]</sup> Today it is a legacy system, and several NSA stations are closing.<sup>[57]</sup>

NSA/CSS, in combination with the equivalent agencies in the United Kingdom (Government Communications Headquarters), Canada (Communications Security Establishment), Australia (Australian Signals Directorate), and New Zealand (Government Communications Security Bureau), otherwise known as the UKUSA group,<sup>[58]</sup> was reported to be in command of the operation of the so-called ECHELON system. Its capabilities were suspected to include the ability to monitor a large proportion of the world's transmitted civilian telephone, fax and data traffic.<sup>[59]</sup>

During the early 1970s, the first of what became more than eight large satellite communications dishes were installed at Menwith Hill.<sup>[60]</sup> Investigative journalist Duncan Campbell reported in 1988 on the "ECHELON" surveillance program, an extension of the UKUSA Agreement on global signals intelligence SIGINT, and detailed how the eavesdropping operations worked.<sup>[61]</sup> On November 3, 1999 the BBC reported that they had confirmation from the Australian Government of the existence of a powerful "global spying network" code-named Echelon, that could "eavesdrop on every single phone call, fax or e-mail, anywhere on the planet" with Britain and the United States as the chief protagonists. They confirmed that Menwith Hill was "linked directly to the headquarters of the US National Security Agency (NSA) at Fort Meade in Maryland".<sup>[62]</sup>

NSA's United States Signals Intelligence Directive 18 (USSID 18) strictly prohibited the interception or collection of information about "... U.S. persons, entities, corporations or organizations...." without explicit written legal permission from the United States Attorney General when the subject is located abroad, or the Foreign Intelligence Surveillance Court when within U.S. borders. Alleged Echelon-related activities, including its use for motives other than national security, including political and industrial espionage, received criticism from countries outside the UKUSA alliance.<sup>[63]</sup>

## Other SIGINT operations overseas

The NSA was also involved in planning to blackmail people with "SEXINT", intelligence gained about a potential target's sexual activity and preferences. Those targeted had not committed any apparent crime nor were they charged with one.<sup>[64]</sup>

In order to support its facial recognition program, the NSA is intercepting "millions of images per day".<sup>[65]</sup>

The Real Time Regional Gateway is a data collection program introduced in 2005 in Iraq by NSA during the Iraq War that consisted of gathering all electronic communication, storing it, then searching and otherwise analyzing it. It was effective in providing information about Iraqi insurgents who had eluded less comprehensive techniques.<sup>[66]</sup> This "collect it all" strategy introduced by NSA director, Keith B. Alexander, is believed by Glenn Greenwald of *The Guardian* to be the model for the comprehensive worldwide mass archiving of communications which NSA is engaged in as of 2013.<sup>[67]</sup>

A dedicated unit of the NSA locates targets for the CIA for extrajudicial assassination in the Middle East.<sup>[68]</sup> The NSA has also spied extensively on the European Union, the United Nations and numerous governments including allies and trading partners in Europe, South America and Asia.<sup>[69][70]</sup>

In June 2015, WikiLeaks published documents showing that NSA spied on French companies.<sup>[71]</sup>

In July 2015, WikiLeaks published documents showing that NSA spied on federal German ministries since the 1990s.<sup>[72][73]</sup> Even Germany's Chancellor Angela Merkel's cellphones and phone of her predecessors had been intercepted.<sup>[74]</sup>



Protesters against NSA data mining in Berlin wearing Chelsea Manning and Edward Snowden masks

## Boundless Informant

Edward Snowden revealed in June 2013 that between February 8 and March 8, 2013, the NSA collected about 124.8 billion telephone data items and 97.1 billion computer data items throughout the world, as was displayed in charts from an internal NSA tool codenamed Boundless Informant. Initially, it was reported that some of these data reflected eavesdropping on citizens in countries like Germany, Spain and France,<sup>[75]</sup> but later on, it became clear that those data were collected by European agencies during military missions abroad and were subsequently shared with NSA.

## Bypassing encryption

In 2013, reporters uncovered a secret memo that claims the NSA created and pushed for the adoption of the Dual EC DRBG encryption standard that contained built-in vulnerabilities in 2006 to the United States National Institute of Standards and Technology (NIST), and the International Organization for Standardization (aka ISO).<sup>[76][77]</sup> This memo appears to give credence to previous speculation by cryptographers at Microsoft Research.<sup>[78]</sup> Edward Snowden claims that the NSA often bypasses encryption altogether by lifting information before it is encrypted or after it is decrypted.<sup>[77]</sup>

XKeyscore rules (as specified in a file xkeyscorerules100.txt, sourced by German TV stations NDR and WDR, who claim to have excerpts from its source code) reveal that the NSA tracks users of privacy-enhancing software tools, including Tor; an anonymous email service provided by the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in Cambridge, Massachusetts; and readers of the Linux Journal.<sup>[79][80]</sup>

## Software backdoors

Linus Torvalds, the founder of Linux kernel, joked during a LinuxCon keynote on September 18, 2013, that the NSA, who are the founder of SELinux, wanted a backdoor in the kernel.<sup>[81]</sup> However, later, Linus' father, a Member of the European Parliament (MEP), revealed that the NSA actually did this.<sup>[82]</sup>

When my oldest son was asked the same question: "Has he been approached by the NSA about backdoors?" he said "No", but at the same time he nodded. Then he was sort of in the legal free. He had given the right answer, everybody understood that the NSA had approached him.

— Nils Torvalds, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens –  
11th Hearing, 11 November 2013<sup>[83]</sup>

IBM Notes was the first widely adopted software product to use public key cryptography for client–server and server–server authentication and for encryption of data. Until US laws regulating encryption were changed in 2000, IBM and Lotus were prohibited from exporting versions of Notes that supported symmetric encryption keys that were longer than 40 bits. In 1997, Lotus negotiated an agreement with the NSA that allowed the export of a version that supported stronger keys with 64 bits, but 24 of the bits were encrypted with a special key and included in the message to provide a "workload reduction factor" for the NSA. This strengthened the protection for users of Notes outside the US against private-sector industrial espionage, but not against spying by the US government.<sup>[84][85]</sup>

## Boomerang routing

While it is assumed that foreign transmissions terminating in the U.S. (such as a non-U.S. citizen accessing a U.S. website) subject non-U.S. citizens to NSA surveillance, recent research into boomerang routing has raised new concerns about the NSA's ability to surveil the domestic Internet traffic of foreign countries.<sup>[18]</sup> Boomerang routing occurs when an Internet transmission that originates and terminates in a single country transits another. Research at the University of Toronto has suggested that approximately 25% of Canadian domestic traffic may be subject to NSA surveillance activities as a result of the boomerang routing of Canadian Internet service providers.<sup>[18]</sup>

## Hardware implanting

A document included in NSA files released with Glenn Greenwald's book *No Place to Hide* details how the agency's Tailored Access Operations (TAO) and other NSA units gain access to hardware. They intercept routers, servers and other network hardware being shipped to organizations targeted for surveillance and install covert implant firmware onto them before they are delivered. This was described by an NSA manager as "some of the most productive operations in TAO because they preposition access points into hard target networks around the world."<sup>[86]</sup>



Intercepted packages are opened carefully by NSA employees



A "load station" implanting a beacon

Computers seized by the NSA due to interdiction are often modified with a physical device known as Cottonmouth.<sup>[87]</sup> Cottonmouth is a device that can be inserted in the USB port of a computer in order to establish remote access to the targeted machine. According to NSA's Tailored Access Operations (TAO) group implant catalog, after implanting Cottonmouth, the NSA can establish a network bridge "that allows the NSA to load exploit software onto modified computers as well as allowing the NSA to relay commands and data between hardware and software implants."<sup>[88]</sup>

## Domestic collection

NSA's mission, as set forth in Executive Order 12333 in 1981, is to collect information that constitutes "foreign intelligence or counterintelligence" while *not* "acquiring information concerning the domestic activities of United States persons". NSA has declared that it relies on the FBI to collect information on foreign intelligence activities within the borders of the United States, while confining its own activities within the United States to the embassies and missions of foreign nations.<sup>[89]</sup>

The appearance of a 'Domestic Surveillance Directorate' of the NSA was soon exposed as a hoax in 2013.<sup>[90][91]</sup>

NSA's domestic surveillance activities are limited by the requirements imposed by the Fourth Amendment to the U.S. Constitution. The Foreign Intelligence Surveillance Court for example held in October 2011, citing multiple Supreme Court precedents, that the Fourth Amendment prohibitions against unreasonable searches and seizures apply to the contents of all communications, whatever the means, because "a person's private communications are akin to personal papers."<sup>[92]</sup> However, these protections do not apply to non-U.S. persons located outside of U.S. borders, so the NSA's foreign surveillance efforts are subject to far fewer limitations under U.S. law.<sup>[93]</sup> The specific requirements for domestic surveillance operations are contained in the Foreign Intelligence Surveillance Act of 1978 (FISA), which does not extend protection to non-U.S. citizens located outside of U.S. territory.<sup>[93]</sup>

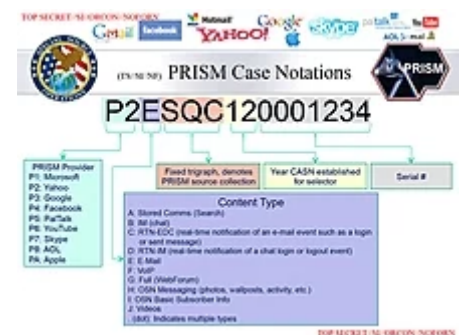
## President's Surveillance Program

George W. Bush, president during the 9/11 terrorist attacks, approved the Patriot Act shortly after the attacks to take anti-terrorist security measures. Title 1, 2, and 9 specifically authorized measures that would be taken by the NSA. These titles granted enhanced domestic security against terrorism, surveillance procedures, and improved intelligence, respectively. On March 10, 2004, there was a debate between President Bush and White House Counsel Alberto Gonzales, Attorney General John Ashcroft, and Acting Attorney General James Comey. The Attorneys General were unsure if the NSA's programs could be considered constitutional. They threatened to resign over the matter, but ultimately the NSA's programs continued.<sup>[94]</sup> On March 11, 2004, President Bush signed a new authorization for mass surveillance of Internet records, in addition to the surveillance of phone records. This allowed the president to be able to override laws such as the Foreign Intelligence Surveillance Act, which protected civilians from mass surveillance. In addition to this, President Bush also signed that the measures of mass surveillance were also retroactively in place.<sup>[95]</sup>

## The PRISM program

Under the PRISM program, which started in 2007,<sup>[96][97]</sup> NSA gathers Internet communications from foreign targets from nine major U.S. Internet-based communication service providers: Microsoft,<sup>[98]</sup> Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. Data gathered include email, videos, photos, VoIP chats such as Skype, and file transfers.

Former NSA director General Keith Alexander claimed that in September 2009 the NSA prevented Najibullah Zazi and his friends from carrying out a terrorist attack.<sup>[99]</sup> However, this claim has been debunked and no evidence has been presented demonstrating that the NSA has ever been instrumental in preventing a terrorist attack.<sup>[100][101][102][103]</sup>



PRISM: a clandestine surveillance program under which the NSA collects user data from companies like Microsoft and Facebook.

## Hacking operations

Besides the more traditional ways of eavesdropping in order to collect signals intelligence, NSA is also engaged in hacking computers, smartphones and their networks. These operations are conducted by the Tailored Access Operations (TAO) division, which has been active since at least circa 1998.<sup>[104]</sup>

According to the *Foreign Policy* magazine, "... the Office of Tailored Access Operations, or TAO, has successfully penetrated Chinese computer and telecommunications systems for almost 15 years, generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China."<sup>[105][106]</sup>

In an interview with *Wired* magazine, Edward Snowden said the Tailored Access Operations division accidentally caused Syria's internet blackout in 2012.<sup>[107]</sup>

## Organizational structure

The NSA is led by the Director of the National Security Agency (DIRNSA), who also serves as Chief of the Central Security Service (CHCSS) and Commander of the United States Cyber Command (USCYBERCOM) and is the highest-ranking military official of these organizations. He is assisted by a Deputy Director, who is the highest-ranking civilian within the NSA/CSS.

NSA also has an Inspector General, head of the Office of the Inspector General (OIG), a General Counsel, head of the Office of the General Counsel (OGC) and a Director of Compliance, who is head of the Office of the Director of Compliance (ODOC).<sup>[108]</sup>

Unlike other intelligence organizations such as the CIA or DIA, NSA has always been particularly reticent concerning its internal organizational structure.

As of the mid-1990s, the National Security Agency was organized into five Directorates:

- The Operations Directorate, which was responsible for SIGINT collection and processing.
- The Technology and Systems Directorate, which develops new technologies for SIGINT collection and processing.
- The Information Systems Security Directorate, which was responsible for NSA's communications and information security missions.
- The Plans, Policy and Programs Directorate, which provided staff support and general direction for the Agency.
- The Support Services Directorate, which provided logistical and administrative support activities.<sup>[109]</sup>



Paul M. Nakasone, the director of the NSA.

Each of these directorates consisted of several groups or elements, designated by a letter. There were for example the A Group, which was responsible for all SIGINT operations against the Soviet Union and Eastern Europe, and G Group, which was responsible for SIGINT related to all non-communist countries. These groups were divided into units designated by an additional number, like unit A5 for breaking Soviet codes, and G6, being the office for the Middle East, North Africa, Cuba, Central and South America.<sup>[110][111]</sup>

## Directorates

As of 2013, NSA has about a dozen directorates, which are designated by a letter, although not all of them are publicly known.<sup>[112]</sup>

In the year 2000, a leadership team was formed, consisting of the Director, the Deputy Director and the Directors of the Signals Intelligence (SID), the Information Assurance (IAD) and the Technical Directorate (TD). The chiefs of other main NSA divisions became associate directors of the senior leadership team.<sup>[113]</sup>

After president George W. Bush initiated the President's Surveillance Program (PSP) in 2001, the NSA created a 24-hour Metadata Analysis Center (MAC), followed in 2004 by the Advanced Analysis Division (AAD), with the mission of analyzing content, Internet metadata and telephone metadata. Both units were part of the Signals Intelligence Directorate.<sup>[114]</sup>

A 2016 proposal would combine the Signals Intelligence Directorate with Information Assurance Directorate into Directorate of Operations.<sup>[115]</sup>

## NSANet

NSANet stands for National Security Agency Network and is the official NSA intranet.<sup>[116]</sup> It is a classified network,<sup>[117]</sup> for information up to the level of TS/SCI<sup>[118]</sup> to support the use and sharing of intelligence data between NSA and the signals intelligence agencies of the four other nations of the Five Eyes partnership. The management of NSANet has been delegated to the Central Security Service Texas (CSSTEXAS).<sup>[119]</sup>

NSANet is a highly secured computer network consisting of fiber-optic and satellite communication channels which are almost completely separated from the public Internet. The network allows NSA personnel and civilian and military intelligence analysts anywhere in the world to have access to the agency's systems and databases. This access is tightly controlled and monitored. For example, every keystroke is logged, activities are audited at random and downloading and printing of documents from NSANet are recorded.<sup>[120]</sup>

In 1998, NSANet, along with NIPRNET and SIPRNET, had "significant problems with poor search capabilities, unorganized data and old information".<sup>[121]</sup> In 2004, the network was reported to have used over twenty commercial off-the-shelf operating systems.<sup>[122]</sup> Some universities that do highly sensitive research are allowed to connect to it.<sup>[123]</sup>

The thousands of Top Secret internal NSA documents that were taken by Edward Snowden in 2013 were stored in "a file-sharing location on the NSA's intranet site"; so, they could easily be read online by NSA personnel. Everyone with a TS/SCI-clearance had access to these documents. As a system administrator, Snowden was responsible for moving accidentally misplaced highly sensitive documents to safer storage locations.<sup>[124]</sup>

## Watch centers

The NSA maintains at least two watch centers:

- National Security Operations Center (NSOC), which is the NSA's current operations center and focal point for time-sensitive SIGINT reporting for the United States SIGINT System (USSS). This center was established in 1968 as the National SIGINT Watch Center (NSWC) and renamed into National SIGINT Operations Center (NSOC) in 1973. This "nerve center of the NSA" got its current name in 1996.<sup>[125]</sup>
- NSA/CSS Threat Operations Center (NTOC), which is the primary NSA/CSS partner for Department of Homeland Security response to cyber incidents. The NTOC establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity and enable the coordination of Computer Network Operations. The NTOC was established in 2004 as a joint Information Assurance and Signals Intelligence project.<sup>[126]</sup>

## Employees

The number of NSA employees is officially classified<sup>[4]</sup> but there are several sources providing estimates. In 1961, NSA had 59,000 military and civilian employees, which grew to 93,067 in 1969, of which 19,300 worked at the headquarters at Fort Meade. In the early 1980s, NSA had roughly 50,000 military and civilian



*Behind the Green Door – Secure communications room with separate computer terminals for access to SIPRNET, GWAN, NSANET, and JWICS*

personnel. By 1989 this number had grown again to 75,000, of which 25,000 worked at the NSA headquarters. Between 1990 and 1995 the NSA's budget and workforce were cut by one third, which led to a substantial loss of experience.<sup>[127]</sup>

In 2012, the NSA said more than 30,000 employees worked at Fort Meade and other facilities.<sup>[2]</sup> In 2012, John C. Inglis, the deputy director, said that the total number of NSA employees is "somewhere between 37,000 and one billion" as a joke,<sup>[4]</sup> and stated that the agency is "probably the biggest employer of introverts."<sup>[4]</sup> In 2013 *Der Spiegel* stated that the NSA had 40,000 employees.<sup>[5]</sup> More widely, it has been described as the world's largest single employer of mathematicians.<sup>[128]</sup> Some NSA employees form part of the workforce of the National Reconnaissance Office (NRO), the agency that provides the NSA with satellite signals intelligence.

As of 2013 about 1,000 system administrators work for the NSA.<sup>[129]</sup>

## Personnel security

The NSA received criticism early on in 1960 after two agents had defected to the Soviet Union. Investigations by the House Un-American Activities Committee and a special subcommittee of the United States House Committee on Armed Services revealed severe cases of ignorance in personnel security regulations, prompting the former personnel director and the director of security to step down and leading to the adoption of stricter security practices.<sup>[130]</sup> Nonetheless, security breaches reoccurred only a year later when in an issue of *Izvestia* of July 23, 1963, a former NSA employee published several cryptologic secrets.

The very same day, an NSA clerk-messenger committed suicide as ongoing investigations disclosed that he had sold secret information to the Soviets on a regular basis. The reluctance of Congressional houses to look into these affairs had prompted a journalist to write, "If a similar series of tragic blunders occurred in any ordinary agency of Government an aroused public would insist that those responsible be officially censured, demoted, or fired." David Kahn criticized the NSA's tactics of concealing its doings as smug and the Congress' blind faith in the agency's right-doing as shortsighted, and pointed out the necessity of surveillance by the Congress to prevent abuse of power.<sup>[130]</sup>

Edward Snowden's leaking of the existence of PRISM in 2013 caused the NSA to institute a "two-man rule", where two system administrators are required to be present when one accesses certain sensitive information.<sup>[129]</sup> Snowden claims he suggested such a rule in 2009.<sup>[131]</sup>

## Polygraphing

The NSA conducts polygraph tests of employees. For new employees, the tests are meant to discover enemy spies who are applying to the NSA and to uncover any information that could make an applicant pliant to coercion.<sup>[132]</sup> As part of the latter, historically *EPQs* or "embarrassing personal questions" about sexual behavior had been included in the NSA polygraph.<sup>[132]</sup> The NSA also conducts five-year periodic reinvestigation polygraphs of employees, focusing on counterintelligence programs. In addition the NSA conducts periodic polygraph investigations in order to find spies and leakers; those who refuse to take them may receive "termination of employment", according to a 1982 memorandum from the director of the NSA.<sup>[133]</sup>



Defense Security Service (DSS) polygraph brochure given to NSA applicants



[Play media](#)

NSA-produced video on the polygraph process

There are also "special access examination" polygraphs for employees who wish to work in highly sensitive areas, and those polygraphs cover counterintelligence questions and some questions about behavior.<sup>[133]</sup> NSA's brochure states that the average test length is between two and four hours.<sup>[134]</sup> A 1983 report of the Office of Technology Assessment stated that "It appears that the NSA [National Security Agency] (and possibly CIA) use the polygraph not to determine deception or truthfulness per se, but as a technique of interrogation to encourage admissions."<sup>[135]</sup> Sometimes applicants in the polygraph process confess to committing felonies such as murder, rape, and selling of illegal drugs. Between 1974 and 1979, of the 20,511 job applicants who took polygraph tests, 695 (3.4%) confessed to previous felony crimes; almost all of those crimes had

been undetected.<sup>[132]</sup>

In 2010 the NSA produced a video explaining its polygraph process.<sup>[136]</sup> The video, ten minutes long, is titled "The Truth About the Polygraph" and was posted to the Web site of the Defense Security Service. Jeff Stein of *The Washington Post* said that the video portrays "various applicants, or actors playing them—it's not clear—describing everything bad they had heard about the test, the implication being that none of it is true."<sup>[137]</sup> AntiPolygraph.org argues that the NSA-produced video omits some information about the polygraph process; it produced a video responding to the NSA video.<sup>[136][138]</sup> George Maschke, the founder of the Web site, accused the NSA polygraph video of being "Orwellian".<sup>[137]</sup>

After Edward Snowden revealed his identity in 2013, the NSA began requiring polygraphing of employees once per quarter.<sup>[139]</sup>

## Arbitrary firing

The number of exemptions from legal requirements has been criticized. When in 1964 Congress was hearing a bill giving the director of the NSA the power to fire at will any employee, *The Washington Post* wrote: "This is the very definition of arbitrariness. It means that an employee could be discharged and disgraced on the basis of anonymous allegations without the slightest opportunity to defend himself." Yet, the bill was accepted by an overwhelming majority.<sup>[130]</sup> Also, every person hired to a job in the US after 2007, at any private organization, state or federal government agency, *must* be reported to the New Hire Registry, ostensibly to look for child support evaders, *except* that employees of an intelligence agency may be excluded from reporting if the director deems it necessary for national security reasons.

## Facilities

---

### Headquarters

#### History of headquarters

When the agency was first established, its headquarters and cryptographic center were in the Naval Security Station in Washington, D.C. The COMINT functions were located in Arlington Hall in Northern Virginia, which served as the headquarters of the U.S. Army's cryptographic operations.<sup>[140]</sup> Because the Soviet Union had detonated a nuclear bomb and because the facilities were crowded, the federal government wanted to move several agencies, including the AFSA/NSA. A planning committee considered Fort Knox, but Fort

Meade, Maryland, was ultimately chosen as NSA headquarters because it was far enough away from Washington, D.C. in case of a nuclear strike and was close enough so its employees would not have to move their families.<sup>[141]</sup>

Construction of additional buildings began after the agency occupied buildings at Fort Meade in the late 1950s, which they soon outgrew.<sup>[141]</sup> In 1963 the new headquarters building, nine stories tall, opened. NSA workers referred to the building as the "Headquarters Building" and since the NSA management occupied the top floor, workers used "Ninth Floor" to refer to their leaders.<sup>[142]</sup> COMSEC remained in Washington, D.C., until its new building was completed in 1968.<sup>[141]</sup> In September 1986, the Operations 2A and 2B buildings, both copper-shielded to prevent eavesdropping, opened with a dedication by President Ronald Reagan.<sup>[143]</sup> The four NSA buildings became known as the "Big Four."<sup>[143]</sup> The NSA director moved to 2B when it opened.<sup>[143]</sup>

Headquarters for the National Security Agency is located at 39°6'32"N 76°46'17"W in Fort George G. Meade, Maryland, although it is separate from other compounds and agencies that are based within this same military installation. Fort Meade is about 20 mi (32 km) southwest of Baltimore,<sup>[144]</sup> and 25 mi (40 km) northeast of Washington, D.C.<sup>[145]</sup> The NSA has two dedicated exits off Baltimore–Washington Parkway. The Eastbound exit from the Parkway (heading toward Baltimore) is open to the public and provides employee access to its main campus and public access to the National Cryptology Museum. The Westbound side exit, (heading toward Washington) is labeled "NSA Employees Only".<sup>[146][147]</sup> The exit may only be used by people with the proper clearances, and security vehicles parked along the road guard the entrance.<sup>[148]</sup>

NSA is the largest employer in the state of Maryland, and two-thirds of its personnel work at Fort Meade.<sup>[149]</sup> Built on 350 acres (140 ha; 0.55 sq mi)<sup>[150]</sup> of Fort Meade's 5,000 acres (2,000 ha; 7.8 sq mi),<sup>[151]</sup> the site has 1,300 buildings and an estimated 18,000 parking spaces.<sup>[145][152]</sup>

The main NSA headquarters and operations building is what James Bamford, author of *Body of Secrets*, describes as "a modern boxy structure" that appears similar to "any stylish office building."<sup>[153]</sup> The building is covered with one-way dark glass, which is lined with copper shielding in order to prevent espionage by trapping in signals and sounds.<sup>[153]</sup> It contains 3,000,000 square feet (280,000 m<sup>2</sup>), or more than 68 acres (28 ha), of floor space; Bamford said that the U.S. Capitol "could easily fit inside it four times over."<sup>[153]</sup>

The facility has over 100 watchposts,<sup>[154]</sup> one of them being the visitor control center, a two-story area that serves as the entrance.<sup>[153]</sup> At the entrance, a white pentagonal structure,<sup>[155]</sup> visitor badges are issued to visitors and security clearances of employees are checked.<sup>[156]</sup> The visitor center includes a painting of the NSA seal.<sup>[155]</sup>



Headquarters at Fort Meade circa 1950s



National Security Agency headquarters in Fort Meade, 2013



NSA headquarters building in Fort Meade (left), NSOC (right)

The OPS2A building, the tallest building in the NSA complex and the location of much of the agency's operations directorate, is accessible from the visitor center. Bamford described it as a "dark glass Rubik's Cube".<sup>[157]</sup> The facility's "red corridor" houses non-security operations such as concessions and the drug store. The name refers to the "red badge" which is worn by someone without a security clearance. The NSA headquarters includes a cafeteria, a credit union, ticket counters for airlines and entertainment, a barbershop, and a bank.<sup>[155]</sup> NSA headquarters has its own post office, fire department, and police force.<sup>[158][159][160]</sup>

The employees at the NSA headquarters reside in various places in the Baltimore-Washington area, including Annapolis, Baltimore, and Columbia in Maryland and the District of Columbia, including the Georgetown community.<sup>[161]</sup> The NSA maintains a shuttle service from the Odenton station of MARC to its Visitor Control Center and has done so since 2005.<sup>[162]</sup>

## Power consumption

Following a major power outage in 2000, in 2003, and in follow-ups through 2007, *The Baltimore Sun* reported that the NSA was at risk of electrical overload because of insufficient internal electrical infrastructure at Fort Meade to support the amount of equipment being installed. This problem was apparently recognized in the 1990s but not made a priority, and "now the agency's ability to keep its operations going is threatened."<sup>[163]</sup>

On August 6, 2006, *The Baltimore Sun* reported that the NSA had completely maxed out the grid, and that Baltimore Gas & Electric (BGE, now Constellation Energy) was unable to sell them any more power.<sup>[164]</sup> NSA decided to move some of its operations to a new satellite facility.



Due to massive amounts of data processing, NSA is the largest electricity consumer in Maryland.<sup>[149]</sup>

BGE provided NSA with 65 to 75 megawatts at Fort Meade in 2007, and expected that an increase of 10 to 15 megawatts would be needed later that year.<sup>[165]</sup> In 2011, the NSA was Maryland's largest consumer of power.<sup>[149]</sup> In 2007, as BGE's largest customer, NSA bought as much electricity as Annapolis, the capital city of Maryland.<sup>[163]</sup>

One estimate put the potential for power consumption by the new Utah Data Center at US\$40 million per year.<sup>[166]</sup>

## Computing assets

In 1995, *The Baltimore Sun* reported that the NSA is the owner of the single largest group of supercomputers.<sup>[167]</sup>

NSA held a groundbreaking ceremony at Fort Meade in May 2013 for its High Performance Computing Center 2, expected to open in 2016.<sup>[168]</sup> Called Site M, the center has a 150 megawatt power substation, 14 administrative buildings and 10 parking garages.<sup>[158]</sup> It cost \$3.2 billion and covers 227 acres (92 ha; 0.355 sq mi).<sup>[158]</sup> The center is 1,800,000 square feet (17 ha; 0.065 sq mi)<sup>[158]</sup> and initially uses 60 megawatts of electricity.<sup>[169]</sup>

Increments II and III are expected to be completed by 2030, and would quadruple the space, covering 5,800,000 square feet (54 ha; 0.21 sq mi) with 60 buildings and 40 parking garages.<sup>[158]</sup> Defense contractors are also establishing or expanding cybersecurity facilities near the NSA and around the Washington metropolitan area.<sup>[158]</sup>

## National Computer Security Center

The DoD Computer Security Center was founded in 1981 and renamed the National Computer Security Center (NCSC) in 1985. NCSC was responsible for computer security throughout the federal government.<sup>[170]</sup> NCSC was part of NSA,<sup>[171]</sup> and during the late 1980s and the 1990s, NSA and NCSC published Trusted Computer System Evaluation Criteria in a six-foot high Rainbow Series of books that detailed trusted computing and network platform specifications.<sup>[172]</sup> The Rainbow books were replaced by the Common Criteria, however, in the early 2000s.<sup>[172]</sup>

## Other U.S. facilities

As of 2012, NSA collected intelligence from four geostationary satellites.<sup>[166]</sup> Satellite receivers were at Roaring Creek Station in Catawissa, Pennsylvania and Salt Creek Station in Arbuckle, California.<sup>[166]</sup> It operated ten to twenty taps on U.S. telecom switches. NSA had installations in several U.S. states and from them observed intercepts from Europe, the Middle East, North Africa, Latin America, and Asia.<sup>[166]</sup>

NSA had facilities at Friendship Annex (FANX) in Linthicum, Maryland, which is a 20 to 25-minute drive from Fort Meade;<sup>[173]</sup> the Aerospace Data Facility at Buckley Air Force Base in Aurora outside Denver, Colorado; NSA Texas in the Texas Cryptology Center at Lackland Air Force Base in San Antonio, Texas; NSA Georgia at Fort Gordon in Augusta, Georgia; NSA Hawaii in Honolulu; the Multiprogram Research Facility in Oak Ridge, Tennessee, and elsewhere.<sup>[161][166]</sup>

On January 6, 2011, a groundbreaking ceremony was held to begin construction on NSA's first Comprehensive National Cyber-security Initiative (CNCI) Data Center, known as the "Utah Data Center" for short. The \$1.5B data center is being built at Camp Williams, Utah, located 25 miles (40 km) south of Salt Lake City, and will help support the agency's National Cyber-security Initiative.<sup>[174]</sup> It is expected to be operational by September 2013.<sup>[166]</sup> Construction of Utah Data Center finished in May 2019.<sup>[175]</sup>

In 2009, to protect its assets and access more electricity, NSA sought to decentralize and expand its existing facilities in Fort Meade and Menwith Hill,<sup>[176]</sup> the latter expansion expected to be completed by 2015.<sup>[177]</sup>

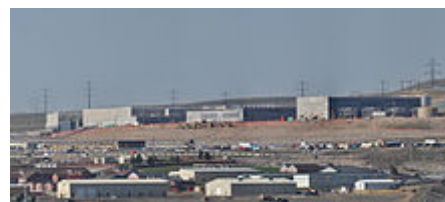
The Yakima Herald-Republic cited Bamford, saying that many of NSA's bases for its Echelon program were a legacy system, using outdated, 1990s technology.<sup>[57]</sup> In 2004, NSA closed its operations at Bad Aibling Station (Field Station 81) in Bad Aibling, Germany.<sup>[178]</sup> In 2012, NSA began to move some of its operations at Yakima Research Station, Yakima Training Center, in Washington state to Colorado, planning to leave Yakima closed.<sup>[179]</sup> As of 2013, NSA also intended to close operations at Sugar Grove, West Virginia.<sup>[57]</sup>

## International stations

Following the signing in 1946–1956<sup>[180]</sup> of the UKUSA Agreement between the United States, United Kingdom, Canada, Australia and New Zealand, who then cooperated on signals intelligence and ECHELON,<sup>[181]</sup> NSA stations were built at GCHQ Bude in Morwenstow, United Kingdom; Geraldton, Pine



Buckley Air Force Base in Colorado



Utah Data Center

Gap and Shoal Bay, Australia; Leitrim and Ottawa, Ontario, Canada; Misawa, Japan; and Waihopai and Tangimoana,<sup>[182]</sup> New Zealand.<sup>[183]</sup>

NSA operates RAF Menwith Hill in North Yorkshire, United Kingdom, which was, according to BBC News in 2007, the largest electronic monitoring station in the world.<sup>[184]</sup> Planned in 1954, and opened in 1960, the base covered 562 acres (227 ha; 0.878 sq mi) in 1999.<sup>[185]</sup>

The agency's European Cryptologic Center (ECC), with 240 employees in 2011, is headquartered at a US military compound in Griesheim, near Frankfurt in Germany. A 2011 NSA report indicates that the ECC is responsible for the "largest analysis and productivity in Europe" and focuses on various priorities, including Africa, Europe, the Middle East and counterterrorism operations.<sup>[186]</sup>

In 2013, a new Consolidated Intelligence Center, also to be used by NSA, is being built at the headquarters of the United States Army Europe in Wiesbaden, Germany.<sup>[187]</sup> NSA's partnership with Bundesnachrichtendienst (BND), the German foreign intelligence service, was confirmed by BND president Gerhard Schindler.<sup>[187]</sup>

## Thailand

Thailand is a "3rd party partner" of the NSA along with nine other nations.<sup>[188]</sup> These are non-English-speaking countries that have made security agreements for the exchange of SIGINT raw material and end product reports.

Thailand is the site of at least two US SIGINT collection stations. One is at the US Embassy in Bangkok, a joint NSA-CIA Special Collection Service (SCS) unit. It presumably eavesdrops on foreign embassies, governmental communications, and other targets of opportunity.<sup>[189]</sup>

The second installation is a FORNSAT (foreign satellite interception) station in the Thai city of Khon Kaen. It is codenamed INDRA, but has also been referred to as LEMONWOOD.<sup>[189]</sup> The station is approximately 40 hectares (99 acres) in size and consists of a large 3,700–4,600 m<sup>2</sup> (40,000–50,000 ft<sup>2</sup>) operations building on the west side of the ops compound and four radome-enclosed parabolic antennas. Possibly two of the radome-enclosed antennas are used for SATCOM intercept and two antennas used for relaying the intercepted material back to NSA. There is also a PUSHER-type circularly-disposed antenna array (CDAA) just north of the ops compound.<sup>[190][191]</sup>

NSA activated Khon Kaen in October 1979. Its mission was to eavesdrop on the radio traffic of Chinese army and air force units in southern China, especially in and around the city of Kunming in Yunnan Province. In the late 1970s, the base consisted only of a small CDAA antenna array that was remote-controlled via satellite from the NSA listening post at Kunia, Hawaii, and a small force of civilian contractors from Bendix Field Engineering Corp. whose job it was to keep the antenna array and satellite relay facilities up and running 24/7.<sup>[190]</sup>

According to the papers of the late General William Odom, the INDRA facility was upgraded in 1986 with a new British-made PUSHER CDAA antenna as part of an overall upgrade of NSA and Thai SIGINT facilities whose objective was to spy on the neighboring communist nations of Vietnam, Laos, and Cambodia.<sup>[190]</sup>



RAF Menwith Hill has the largest NSA presence in the United Kingdom.<sup>[177]</sup>

The base apparently fell into disrepair in the 1990s as China and Vietnam became more friendly towards the US, and by 2002 archived satellite imagery showed that the PUSHER CDAA antenna had been torn down, perhaps indicating that the base had been closed. At some point in the period since 9/11, the Khon Kaen base was reactivated and expanded to include a sizeable SATCOM intercept mission. It is likely that the NSA presence at Khon Kaen is relatively small, and that most of the work is done by civilian contractors.<sup>[190]</sup>

## Research and development

---

NSA has been involved in debates about public policy, both indirectly as a behind-the-scenes adviser to other departments, and directly during and after Vice Admiral Bobby Ray Inman's directorship. NSA was a major player in the debates of the 1990s regarding the export of cryptography in the United States. Restrictions on export were reduced but not eliminated in 1996.

Its secure government communications work has involved the NSA in numerous technology areas, including the design of specialized communications hardware and software, production of dedicated semiconductors (at the Ft. Meade chip fabrication plant), and advanced cryptography research. For 50 years, NSA designed and built most of its computer equipment in-house, but from the 1990s until about 2003 (when the U.S. Congress curtailed the practice), the agency contracted with the private sector in the fields of research and equipment.<sup>[192]</sup>

## Data Encryption Standard

NSA was embroiled in some controversy concerning its involvement in the creation of the Data Encryption Standard (DES), a standard and public block cipher algorithm used by the U.S. government and banking community.<sup>[193]</sup> During the development of DES by IBM in the 1970s, NSA recommended changes to some details of the design. There was suspicion that these changes had weakened the algorithm sufficiently to enable the agency to eavesdrop if required, including speculation that a critical component—the so-called S-boxes—had been altered to insert a "backdoor" and that the reduction in key length might have made it feasible for NSA to discover DES keys using massive computing power. It has since been observed that the S-boxes in DES are particularly resilient against differential cryptanalysis, a technique which was not publicly discovered until the late 1980s but known to the IBM DES team.

## Advanced Encryption Standard

The involvement of NSA in selecting a successor to Data Encryption Standard (DES), the Advanced Encryption Standard (AES), was limited to hardware performance testing (see AES competition).<sup>[194]</sup> NSA has subsequently certified AES for protection of classified information when used in NSA-approved systems.<sup>[195]</sup>

## NSA encryption systems

The NSA is responsible for the encryption-related components in these legacy systems:



FROSTBURG was the NSA's first supercomputer, used from 1991 to 1997

- FNBDT Future Narrow Band Digital Terminal<sup>[196]</sup>
- KL-7 ADONIS off-line rotor encryption machine (post-WWII – 1980s)<sup>[197][198]</sup>
- KW-26 ROMULUS electronic in-line teletypewriter encryptor (1960s–1980s)<sup>[199]</sup>
- KW-37 JASON fleet broadcast encryptor (1960s–1990s)<sup>[198]</sup>
- KY-57 VINSON tactical radio voice encryptor<sup>[199]</sup>
- KG-84 Dedicated Data Encryption/Decryption<sup>[199]</sup>
- STU-III secure telephone unit,<sup>[199]</sup> phased out by the STE<sup>[200]</sup>



STU-III secure telephones on display at the National Cryptologic Museum

The NSA oversees encryption in the following systems that are in use today:

- EKMS Electronic Key Management System<sup>[201]</sup>
- Fortezza encryption based on portable crypto token in PC Card format<sup>[202]</sup>
- SINCGARS tactical radio with cryptographically controlled frequency hopping<sup>[203]</sup>
- STE secure terminal equipment<sup>[200]</sup>
- TACLANE product line by General Dynamics C4 Systems<sup>[204]</sup>

The NSA has specified Suite A and Suite B cryptographic algorithm suites to be used in U.S. government systems; the Suite B algorithms are a subset of those previously specified by NIST and are expected to serve for most information protection purposes, while the Suite A algorithms are secret and are intended for especially high levels of protection.<sup>[195]</sup>

## SHA

The widely used SHA-1 and SHA-2 hash functions were designed by NSA. SHA-1 is a slight modification of the weaker SHA-0 algorithm, also designed by NSA in 1993. This small modification was suggested by NSA two years later, with no justification other than the fact that it provides additional security. An attack for SHA-0 that does not apply to the revised algorithm was indeed found between 1998 and 2005 by academic cryptographers. Because of weaknesses and key length restrictions in SHA-1, NIST deprecates its use for digital signatures, and approves only the newer SHA-2 algorithms for such applications from 2013 on.<sup>[205]</sup>

A new hash standard, SHA-3, has recently been selected through the competition concluded October 2, 2012 with the selection of Keccak as the algorithm. The process to select SHA-3 was similar to the one held in choosing the AES, but some doubts have been cast over it,<sup>[206][207]</sup> since fundamental modifications have been made to Keccak in order to turn it into a standard.<sup>[208]</sup> These changes potentially undermine the cryptanalysis performed during the competition and reduce the security levels of the algorithm.<sup>[206]</sup>

## Clipper chip

Because of concerns that widespread use of strong cryptography would hamper government use of wiretaps, NSA proposed the concept of key escrow in 1993 and introduced the Clipper chip that would offer stronger protection than DES but would allow access to encrypted data by authorized law enforcement officials.<sup>[209]</sup> The proposal was strongly opposed and key escrow requirements ultimately went nowhere.<sup>[210]</sup> However, NSA's Fortezza hardware-based encryption cards, created for the Clipper project, are still used within government, and NSA ultimately declassified and published the design of the Skipjack cipher used on the cards.<sup>[211][212]</sup>

## Dual\_EC\_DRBG random number generator cryptotrojan

NSA promoted the inclusion of a random number generator called Dual EC DRBG in the U.S. National Institute of Standards and Technology's 2007 guidelines. This led to speculation of a backdoor which would allow NSA access to data encrypted by systems using that pseudorandom number generator (PRNG).<sup>[213]</sup>

This is now deemed to be plausible based on the fact that output of next iterations of PRNG can provably be determined if relation between two internal Elliptic Curve points is known.<sup>[214][215]</sup> Both NIST and RSA are now officially recommending against the use of this PRNG.<sup>[216][217]</sup>

## Perfect Citizen

Perfect Citizen is a program to perform vulnerability assessment by the NSA on U.S. critical infrastructure.<sup>[218][219]</sup> It was originally reported to be a program to develop a system of sensors to detect cyber attacks on critical infrastructure computer networks in both the private and public sector through a network monitoring system named *Einstein*.<sup>[220][221]</sup> It is funded by the Comprehensive National Cybersecurity Initiative and thus far Raytheon has received a contract for up to \$100 million for the initial stage.

## Academic research

NSA has invested many millions of dollars in academic research under grant code prefix *MDA904*, resulting in over 3,000 papers as of October 11, 2007. NSA/CSS has, at times, attempted to restrict the publication of academic research into cryptography; for example, the Khufu and Khafre block ciphers were voluntarily withheld in response to an NSA request to do so. In response to a FOIA lawsuit, in 2013 the NSA released the 643-page research paper titled, "Untangling the Web: A Guide to Internet Research,"<sup>[222]</sup> written and compiled by NSA employees to assist other NSA workers in searching for information of interest to the agency on the public Internet.<sup>[223]</sup>

## Patents

NSA has the ability to file for a patent from the U.S. Patent and Trademark Office under gag order. Unlike normal patents, these are not revealed to the public and do not expire. However, if the Patent Office receives an application for an identical patent from a third party, they will reveal NSA's patent and officially grant it to NSA for the full term on that date.<sup>[224]</sup>

One of NSA's published patents describes a method of geographically locating an individual computer site in an Internet-like network, based on the latency of multiple network connections.<sup>[225]</sup> Although no public patent exists, NSA is reported to have used a similar locating technology called trilateralization that allows real-time tracking of an individual's location, including altitude from ground level, using data obtained from cellphone towers.<sup>[226]</sup>

## Insignia and memorials

The heraldic insignia of NSA consists of an eagle inside a circle, grasping a key in its talons.<sup>[227]</sup> The eagle represents the agency's national mission.<sup>[227]</sup> Its breast features a shield with bands of red and white, taken from the Great Seal of the United States and representing Congress.<sup>[227]</sup> The key is taken from the emblem of Saint Peter and represents security.<sup>[227]</sup>

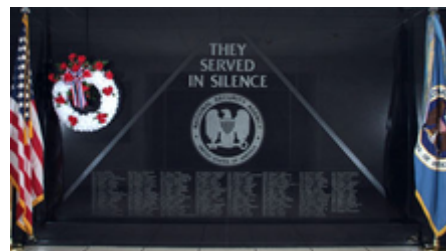


When the NSA was created, the agency had no emblem and used that of the Department of Defense.<sup>[228]</sup> The agency adopted its first of two emblems in 1963.<sup>[228]</sup> The current NSA insignia has been in use since 1965, when then-Director, LTG Marshall S. Carter (USA) ordered the creation of a device to represent the agency.<sup>[229]</sup>

The NSA's flag consists of the agency's seal on a light blue background.

Crews associated with NSA missions have been involved in a number of dangerous and deadly situations.<sup>[230]</sup> The USS Liberty incident in 1967 and USS Pueblo incident in 1968 are examples of the losses endured during the Cold War.<sup>[230]</sup>

The National Security Agency/Central Security Service Cryptologic Memorial honors and remembers the fallen personnel, both military and civilian, of these intelligence missions.<sup>[231]</sup> It is made of black granite, and has 171 names carved into it, as of 2013.<sup>[231]</sup> It is located at NSA headquarters. A tradition of declassifying the stories of the fallen was begun in 2001.<sup>[231]</sup>



National Cryptologic Memorial

## Controversy and litigation

---

In the United States, at least since 2001,<sup>[232]</sup> there has been legal controversy over what signal intelligence can be used for and how much freedom the National Security Agency has to use signal intelligence.<sup>[233]</sup> In 2015, the government made slight changes in how it uses and collects certain types of data,<sup>[234]</sup> specifically phone records. The government was not analyzing the phone records as of early 2019.<sup>[235]</sup> The surveillance programs were deemed unlawful in September 2020 in a court of appeals case.<sup>[52]</sup>

### Warrantless wiretaps

On December 16, 2005, *The New York Times* reported that, under White House pressure and with an executive order from President George W. Bush, the National Security Agency, in an attempt to thwart terrorism, had been tapping phone calls made to persons outside the country, without obtaining warrants from the United States Foreign Intelligence Surveillance Court, a secret court created for that purpose under the Foreign Intelligence Surveillance Act (FISA).<sup>[236]</sup>

One such surveillance program, authorized by the U.S. Signals Intelligence Directive 18 of President George Bush, was the Highlander Project undertaken for the National Security Agency by the U.S. Army 513th Military Intelligence Brigade. NSA relayed telephone (including cell phone) conversations obtained from ground, airborne, and satellite monitoring stations to various U.S. Army Signal Intelligence Officers, including the 201st Military Intelligence Battalion. Conversations of citizens of the U.S. were intercepted, along with those of other nations.<sup>[237]</sup>

Proponents of the surveillance program claim that the President has executive authority to order such action, arguing that laws such as FISA are overridden by the President's Constitutional powers. In addition, some argued that FISA was implicitly overridden by a subsequent statute, the Authorization for Use of Military Force, although the Supreme Court's ruling in *Hamdan v. Rumsfeld* deprecates this view. In the August 2006 case *ACLU v. NSA*, U.S. District Court Judge Anna Diggs Taylor concluded that NSA's warrantless surveillance program was both illegal and unconstitutional. On July 6, 2007, the 6th Circuit Court of Appeals vacated the decision on the grounds that the ACLU lacked standing to bring the suit.<sup>[238]</sup>

On January 17, 2006, the Center for Constitutional Rights filed a lawsuit, CCR v. Bush, against the George W. Bush Presidency. The lawsuit challenged the National Security Agency's (NSA's) surveillance of people within the U.S., including the interception of CCR emails without securing a warrant first.<sup>[239][240]</sup>

In September 2008, the Electronic Frontier Foundation (EFF) filed a class action lawsuit against the NSA and several high-ranking officials of the Bush administration,<sup>[241]</sup> charging an "illegal and unconstitutional program of dragnet communications surveillance,"<sup>[242]</sup> based on documentation provided by former AT&T technician Mark Klein.<sup>[243]</sup>

As a result of the USA Freedom Act passed by Congress in June 2015, the NSA had to shut down its bulk phone surveillance program on November 29 of the same year. The USA Freedom Act forbids the NSA to collect metadata and content of phone calls unless it has a warrant for terrorism investigation. In that case, the agency must ask the telecom companies for the record, which will only be kept for six months. The NSA's use of large telecom companies to assist it with its surveillance efforts has caused several privacy concerns.<sup>[244]:1568–69</sup>

## **AT&T Internet monitoring**

In May 2008, Mark Klein, a former AT&T employee, alleged that his company had cooperated with NSA in installing Narus hardware to replace the FBI Carnivore program, to monitor network communications including traffic between U.S. citizens.<sup>[245]</sup>

## **Data mining**

NSA was reported in 2008 to use its computing capability to analyze "transactional" data that it regularly acquires from other government agencies, which gather it under their own jurisdictional authorities. As part of this effort, NSA now monitors huge volumes of records of domestic email data, web addresses from Internet searches, bank transfers, credit-card transactions, travel records, and telephone data, according to current and former intelligence officials interviewed by The Wall Street Journal. The sender, recipient, and subject line of emails can be included, but the content of the messages or of phone calls are not.<sup>[246]</sup>

A 2013 advisory group for the Obama administration, seeking to reform NSA spying programs following the revelations of documents released by Edward J. Snowden.<sup>[247]</sup> mentioned in 'Recommendation 30' on page 37, "...that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application." Retired cybersecurity expert Richard A. Clarke was a group member and stated on April 11, 2014 that NSA had no advance knowledge of Heartbleed.<sup>[248]</sup>

## **Illegally obtained evidence**

In August 2013 it was revealed that a 2005 IRS training document showed that NSA intelligence intercepts and wiretaps, both foreign and domestic, were being supplied to the Drug Enforcement Administration (DEA) and Internal Revenue Service (IRS) and were illegally used to launch criminal investigations of US citizens. Law enforcement agents were directed to conceal how the investigations began and recreate an apparently legal investigative trail by re-obtaining the same evidence by other means.<sup>[249][250]</sup>

## **Barack Obama administration**

In the months leading to April 2009, the NSA intercepted the communications of U.S. citizens, including a Congressman, although the Justice Department believed that the interception was unintentional. The Justice Department then took action to correct the issues and bring the program into compliance with existing laws.<sup>[251]</sup> United States Attorney General Eric Holder resumed the program according to his understanding of the Foreign Intelligence Surveillance Act amendment of 2008, without explaining what had occurred.<sup>[252]</sup>

Polls conducted in June 2013 found divided results among Americans regarding NSA's secret data collection.<sup>[253]</sup> Rasmussen Reports found that 59% of Americans disapprove,<sup>[254]</sup> Gallup found that 53% disapprove,<sup>[255]</sup> and Pew found that 56% are in favor of NSA data collection.<sup>[256]</sup>

## Section 215 metadata collection

On April 25, 2013, the NSA obtained a court order requiring Verizon's Business Network Services to provide metadata on all calls in its system to the NSA "on an ongoing daily basis" for a three-month period, as reported by The Guardian on June 6, 2013. This information includes "the numbers of both parties on a call ... location data, call duration, unique identifiers, and the time and duration of all calls" but not "[t]he contents of the conversation itself". The order relies on the so-called "business records" provision of the Patriot Act.<sup>[257][258]</sup>

In August 2013, following the Snowden leaks, new details about the NSA's data mining activity were revealed. Reportedly, the majority of emails into or out of the United States are captured at "selected communications links" and automatically analyzed for keywords or other "selectors". Emails that do not match are deleted.<sup>[259]</sup>

The utility of such a massive metadata collection in preventing terrorist attacks is disputed. Many studies reveal the dragnet like system to be ineffective. One such report, released by the New America Foundation concluded that after an analysis of 225 terrorism cases, the NSA "had no discernible impact on preventing acts of terrorism."<sup>[260]</sup>

Defenders of the program said that while metadata alone cannot provide all the information necessary to prevent an attack, it assures the ability to "connect the dots"<sup>[261]</sup> between suspect foreign numbers and domestic numbers with a speed only the NSA's software is capable of. One benefit of this is quickly being able to determine the difference between suspicious activity and real threats.<sup>[262]</sup> As an example, NSA director General Keith B. Alexander mentioned at the annual Cybersecurity Summit in 2013, that metadata analysis of domestic phone call records after the Boston Marathon bombing helped determine that rumors of a follow-up attack in New York were baseless.<sup>[261]</sup>

In addition to doubts about its effectiveness, many people argue that the collection of metadata is an unconstitutional invasion of privacy. As of 2015, the collection process remains legal and grounded in the ruling from Smith v. Maryland (1979). A prominent opponent of the data collection and its legality is U.S. District Judge Richard J. Leon, who issued a report in 2013<sup>[263]</sup> in which he stated: "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval...Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment".

As of May 7, 2015, the United States Court of Appeals for the Second Circuit ruled that the interpretation of Section 215 of the Patriot Act was wrong and that the NSA program that has been collecting Americans' phone records in bulk is illegal.<sup>[264]</sup> It stated that Section 215 cannot be clearly interpreted to allow government to collect national phone data and, as a result, expired on June 1, 2015. This ruling "is the first time a higher-level court in the regular judicial system has reviewed the N.S.A. phone records program."<sup>[265]</sup> The replacement law known as the USA Freedom Act, which will enable the NSA to continue to have bulk access to citizens' metadata but with the stipulation that the data will now be stored by the companies

themselves.<sup>[265]</sup> This change will not have any effect on other Agency procedures - outside of metadata collection - which have purportedly challenged Americans' Fourth Amendment rights;<sup>[266]</sup> including Upstream collection, a mass of techniques used by the Agency to collect and store American's data/communications directly from the Internet backbone.<sup>[267]</sup>

Under the Upstream collection program, the NSA paid telecommunications companies hundreds of millions of dollars in order to collect data from them.<sup>[268]</sup> While companies such as Google and Yahoo! claim that they do not provide "direct access" from their servers to the NSA unless under a court order,<sup>[269]</sup> the NSA had access to emails, phone calls and cellular data users.<sup>[270]</sup> Under this new ruling, telecommunications companies maintain bulk user metadata on their servers for at least 18 months, to be provided upon request to the NSA.<sup>[265]</sup> This ruling made the mass storage of specific phone records at NSA datacenters illegal, but it did not rule on Section 215's constitutionality.<sup>[265]</sup>

## Fourth Amendment encroachment

In a declassified document it was revealed that 17,835 phone lines were on an improperly permitted "alert list" from 2006 to 2009 in breach of compliance, which tagged these phone lines for daily monitoring.<sup>[271][272][273]</sup> Eleven percent of these monitored phone lines met the agency's legal standard for "reasonably articulable suspicion" (RAS).<sup>[271][274]</sup>

The NSA tracks the locations of hundreds of millions of cellphones per day, allowing it to map people's movements and relationships in detail.<sup>[275]</sup> The NSA has been reported to have access to all communications made via Google, Microsoft, Facebook, Yahoo, YouTube, AOL, Skype, Apple and Paltalk,<sup>[276]</sup> and collects hundreds of millions of contact lists from personal email and instant messaging accounts each year.<sup>[277]</sup> It has also managed to weaken much of the encryption used on the Internet (by collaborating with, coercing or otherwise infiltrating numerous technology companies to leave "backdoors" into their systems), so that the majority of encryption is inadvertently vulnerable to different forms of attack.<sup>[278][279]</sup>

Domestically, the NSA has been proven to collect and store metadata records of phone calls,<sup>[280]</sup> including over 120 million US Verizon subscribers,<sup>[281]</sup> as well as intercept vast amounts of communications via the internet (Upstream).<sup>[276]</sup> The government's legal standing had been to rely on a secret interpretation of the Patriot Act whereby the entirety of US communications may be considered "relevant" to a terrorism investigation if it is expected that even a tiny minority may relate to terrorism.<sup>[282]</sup> The NSA also supplies foreign intercepts to the DEA, IRS and other law enforcement agencies, who use these to initiate criminal investigations. Federal agents are then instructed to "recreate" the investigative trail via parallel construction.<sup>[283]</sup>

The NSA also spies on influential Muslims to obtain information that could be used to discredit them, such as their use of pornography. The targets, both domestic and abroad, are not suspected of any crime but hold religious or political views deemed "radical" by the NSA.<sup>[284]</sup>

According to a report in *The Washington Post* in July 2014, relying on information provided by Snowden, 90% of those placed under surveillance in the U.S. are ordinary Americans and are not the intended targets. The newspaper said it had examined documents including emails, text messages, and online accounts that support the claim.<sup>[285]</sup>

## Congressional oversight

Despite White House claims that these programs have congressional oversight, many members of Congress were unaware of the existence of these NSA programs or the secret interpretation of the Patriot Act, and have consistently been denied access to basic information about them.<sup>[286]</sup> The United States Foreign Intelligence Surveillance Court, the secret court charged with regulating the NSA's activities is, according to its chief judge, incapable of investigating or verifying how often the NSA breaks even its own secret rules.<sup>[287]</sup> It has since been reported that the NSA violated its own rules on data access thousands of times a year, many of these violations involving large-scale data interceptions.<sup>[288]</sup> NSA officers have even used data intercepts to spy on love interests;<sup>[289]</sup> "most of the NSA violations were self-reported, and each instance resulted in administrative action of termination."<sup>[290]</sup>



[Play media](#)

Excerpt of James Clapper's testimony before the Senate Select Committee on Intelligence

The NSA has "generally disregarded the special rules for disseminating United States person information" by illegally sharing its intercepts with other law enforcement agencies.<sup>[291]</sup> A March 2009 FISA Court opinion, which the court released, states that protocols restricting data queries had been "so frequently and systemically violated that it can be fairly said that this critical element of the overall ... regime has never functioned effectively."<sup>[292][293]</sup> In 2011 the same court noted that the "volume and nature" of the NSA's bulk foreign Internet intercepts was "fundamentally different from what the court had been led to believe".<sup>[291]</sup> Email contact lists (including those of US citizens) are collected at numerous foreign locations to work around the illegality of doing so on US soil.<sup>[277]</sup>

Legal opinions on the NSA's bulk collection program have differed. In mid-December 2013, U.S. District Judge Richard Leon ruled that the "almost-Orwellian" program likely violates the Constitution, and wrote, "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on 'that degree of privacy' that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware 'the abridgement of freedom of the people by gradual and silent encroachments by those in power,' would be aghast."<sup>[294]</sup>

Later that month, U.S. District Judge William Pauley ruled that the NSA's collection of telephone records is legal and valuable in the fight against terrorism. In his opinion, he wrote, "a bulk telephony metadata collection program [is] a wide net that could find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data" and noted that a similar collection of data prior to 9/11 might have prevented the attack.<sup>[295]</sup>

## Official responses

At a March 2013 Senate Intelligence Committee hearing, Senator Ron Wyden asked Director of National Intelligence James Clapper, "does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper replied "No, sir. ... Not wittingly. There are cases where they could inadvertently perhaps collect, but not wittingly."<sup>[296]</sup> This statement came under scrutiny months later, in June 2013, details of the PRISM surveillance program were published, showing that "the NSA apparently can gain access to the servers of nine Internet companies for a wide range of digital data."<sup>[296]</sup> Wyden said that Clapper had failed to give a "straight answer" in his testimony. Clapper, in response to criticism, said, "I responded in what I thought was the most truthful, or least untruthful manner." Clapper added, "There are honest differences on the semantics of what -- when someone says 'collection' to me, that has a specific meaning, which may have a different meaning to him."<sup>[296]</sup>

NSA whistle-blower Edward Snowden additionally revealed the existence of XKeyscore, a top secret NSA program that allows the agency to search vast databases of "the metadata as well as the content of emails and other internet activity, such as browser history," with capability to search by "name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used."<sup>[297]</sup> XKeyscore "provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst."<sup>[297]</sup>

Regarding the necessity of these NSA programs, Alexander stated on June 27 2013 that the NSA's bulk phone and Internet intercepts had been instrumental in preventing 54 terrorist "events", including 13 in the US, and in all but one of these cases had provided the initial tip to "unravel the threat stream".<sup>[298]</sup> On July 31 NSA Deputy Director John Inglis conceded to the Senate that these intercepts had not been vital in stopping any terrorist attacks, but were "close" to vital in identifying and convicting four San Diego men for sending US\$8,930 to Al-Shabaab, a militia that conducts terrorism in Somalia.<sup>[299][300][301]</sup>

The U.S. government has aggressively sought to dismiss and challenge Fourth Amendment cases raised against it, and has granted retroactive immunity to ISPs and telecoms participating in domestic surveillance.<sup>[302][303]</sup>

The U.S. military has acknowledged blocking access to parts of *The Guardian* website for thousands of defense personnel across the country,<sup>[304][305]</sup> and blocking the entire *Guardian* website for personnel stationed throughout Afghanistan, the Middle East, and South Asia.<sup>[306]</sup>

An October 2014 United Nations report condemned mass surveillance by the United States and other countries as violating multiple international treaties and conventions that guarantee core privacy rights.<sup>[307]</sup>

## **Responsibility for international ransomware attack**

An exploit dubbed EternalBlue, which was claimed to have been created by the NSA by hacker group The Shadow Brokers and whistleblower Edward Snowden, was used in the unprecedented worldwide WannaCry ransomware attack in May 2017. The exploit had been leaked online by a hacking group, The Shadow Brokers, nearly a month prior to the attack. A number of experts have pointed the finger at the NSA's non-disclosure of the underlying vulnerability, and their loss of control over the EternalBlue attack tool that exploited it. Edward Snowden said that if the NSA had "privately disclosed the flaw used to attack hospitals when they found it, not when they lost it, [the attack] might not have happened".<sup>[308]</sup> Wikipedia co-founder, Jimmy Wales, stated that he joined "with Microsoft and the other leaders of the industry in saying this is a huge screw-up by the government ... the moment the NSA found it, they should have notified Microsoft so they could quietly issue a patch and really chivvy people along, long before it became a huge problem."<sup>[309]</sup>

## **2015 Michelle Obama email hack**

Former employee David Evenden, who had left the NSA to work for US defense contractor Cyperpoint at a position in the United Arab Emirates, was tasked with hacking UAE neighbor Qatar in 2015 to determine if they were funding terrorist group Muslim Brotherhood. He quit the company after learning his team had hacked Obama's email exchanges with Qatari Sheikha Moza bint Nasser, just prior to the First Lady's visit to Doha.<sup>[310]</sup> Upon Evenden's return to the US, he reported his experiences to the FBI. The incident highlights a growing trend of former NSA employees and contractors leaving the agency to start up their own firms, and then hiring out to countries like Turkey, Sudan and even Russia, a country involved in numerous cyberattacks against the US.<sup>[310]</sup>

## See also

---

- Australian Signals Directorate (ASD) – Australia
- FAPSI – Russia (1991–2003)
- Garda National Surveillance Unit (NSU) – Ireland
- Ghidra (software)
- Internal Security Department (Singapore) (ISD) – Singapore
- Korean Air Lines Flight 007
- Harold T. Martin III
- Mass surveillance in the United Kingdom
- Ministry of State Security (Stasi) – former German Democratic Republic
- Ministry of State Security (China) (MSS) – China
- National Intelligence Priorities Framework
- National Technical Research Organisation (NTRO) – India
- Operation Ivy Bells
- Operation Eikonal
- Special Communications Service of Russia (Spetssvyaz) – Russia
- Unit 8200—Israel's equivalent to the NSA

## Notes

---

1. Burns, Thomas L. (1990). "The Origins of the National Security Agency" ([https://web.archive.org/web/20160322122158/https://www.nsa.gov/public\\_info/files/cryptologic\\_histories/origins\\_of\\_nsa.pdf](https://web.archive.org/web/20160322122158/https://www.nsa.gov/public_info/files/cryptologic_histories/origins_of_nsa.pdf)) (PDF). United States Cryptologic History. National Security Agency. p. 97. Archived from the original ([https://www.nsa.gov/public\\_info/files/cryptologic\\_histories/origins\\_of\\_nsa.pdf](https://www.nsa.gov/public_info/files/cryptologic_histories/origins_of_nsa.pdf)) (PDF) on March 22, 2016.
2. "60 Years of Defending Our Nation" ([https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF). National Security Agency. 2012. p. 3. Archived from the original ([https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF) on 2013-06-14. Retrieved July 6, 2013. "On November 4, 2012, the National Security Agency (NSA) celebrates its 60th anniversary of providing critical information to U.S. decision makers and Armed Forces personnel in defense of our Nation. NSA has evolved from a staff of approximately 7,600 military and civilian employees housed in 1952 in a vacated school in Arlington, VA, into a workforce of more than 30,000 demographically diverse men and women located at NSA headquarters in Ft. Meade, MD, in four national Cryptologic Centers, and at sites throughout the world."
3. Priest, Dana (July 21, 2013). "NSA growth fueled by need to target terrorists" ([https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html)). *The Washington Post*. Retrieved July 22, 2013. "Since the attacks of Sept. 11, 2001, its civilian and military workforce has grown by one-third, to about 33,000, according to the NSA. Its budget has roughly doubled."
4. "Introverted? Then NSA wants you. (<http://fcw.com/blogs/circuit/2012/04/fedsmc-chris-inglis-federal-workforce.aspx>)" *Florida Championship Wrestling*. April 2012. Retrieved July 1, 2013.
5. Rosenbach, Marcel; Stark, Holger; Stock, Jonathan (June 10, 2013). "Prism Exposed: Data Surveillance with Global Implications" (<http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761.html>). *Spiegel Online*. Spiegel Online International. p. 2. "How can an intelligence agency, even one as large and well-staffed as the NSA with its 40,000 employees, work meaningfully with such a flood of information?"

6. Gellman, Barton; Greg Miller (August 29, 2013). "U.S. spy network's successes, failures and objectives detailed in 'black budget' summary" ([https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972\\_story.html](https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html)). *The Washington Post*. p. 3. Retrieved August 29, 2013.
7. Shane, Scott (August 29, 2013). "New Leaked Document Outlines U.S. Spending on Intelligence Agencies" (<https://www.nytimes.com/2013/08/30/us/politics/leaked-document-outlines-us-spending-on-intelligence.html>). *The New York Times*. Retrieved August 29, 2013.
8. "About NSA: Mission" (<https://www.nsa.gov/about/mission/index.shtml>). National Security Agency. Retrieved September 14, 2014.
9. Ellen Nakashima (January 26, 2008). "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions" ([https://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261\\_pf.html](https://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261_pf.html)). *The Washington Post*. Retrieved February 9, 2008.
10. Executive Order 13470 – 2008 Amendments to Executive Order 12333 (<http://www.gpo.gov/fdsys/pkg/WCPD-2008-08-04/pdf/WCPD-2008-08-04-Pg1064.pdf>), United States Intelligence Activities, July 30, 2008 (PDF)
11. Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, Random House Digital, Inc., December 18, 2007
12. Malkin, Bonnie. "NSA surveillance: US bugged EU offices". *The Daily Telegraph*, June 30, 2013.
13. Ngak, Chenda. "NSA leaker Snowden claimed U.S. and Israel co-wrote Stuxnet virus" (<https://www.cbsnews.com/news/nsa-leaker-snowden-claimed-us-and-israel-co-wrote-stuxnet-virus/>), CBS, July 9, 2013
14. Bamford, James (June 12, 2013). "The Secret War" (<https://web.archive.org/web/20140125144725/http://www.wired.com/threatlevel/?p=58188>). *Wired*. Archived from the original (<https://www.wired.com/threatlevel/?p=58188>) on January 25, 2014.
15. Ann Curry (anchor), John Pike (guest), Pete Williams (guest) and James Bamford (guest) (February 27, 2001). "Congress to Hold Closed Hearings on Accused Spy Robert Hanssen Later This Week" (<http://www.globalsecurity.org/org/news/2001/010227-spy.htm>). *Today*. NBC.
16. Lichtblau, Eric (February 28, 2001). "Spy Suspect May Have Revealed U.S. Bugging; Espionage: Hanssen left signs that he told Russia where top-secret overseas eavesdropping devices are placed, officials say" ([https://web.archive.org/web/20010417230720/http://www.latimes.com/news/nation/updates2/lat\\_spy010228.htm](https://web.archive.org/web/20010417230720/http://www.latimes.com/news/nation/updates2/lat_spy010228.htm)). *Los Angeles Times*. p. A1. Archived from the original ([http://www.latimes.com/news/nation/updates2/lat\\_spy010228.htm](http://www.latimes.com/news/nation/updates2/lat_spy010228.htm)) on April 17, 2001.
17. Executive Order 13470 – 2008 Amendments to Executive Order 12333 (<http://www.gpo.gov/fdsys/pkg/WCPD-2008-08-04/pdf/WCPD-2008-08-04-Pg1064.pdf>), United States Intelligence Activities, Section C.2, July 30, 2008
18. Obar, Jonathan A.; Clement, Andrew (July 1, 2013) [June 5–7, 2012]. Ross, P.; Shtern, J. (eds.). *Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty*. TEM 2013: Proceedings of the Technology & Emerging Media Track – Annual Conference of the Canadian Communication Association. Victoria, British Columbia. doi:10.2139/ssrn.2311792 (<https://doi.org/10.2139%2Fssrn.2311792>). SSRN 2311792 (<https://ssrn.com/abstract=2311792>).
19. "The Black Chamber - Pearl Harbor Review" (<https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/pearl-harbor-review/black-chamber.shtml>). nsa.gov. Retrieved 23 February 2018.
20. "The National Archives, Records of the National Security Agency" (<https://www.archives.gov/research/guide-fed-records/groups/457.html>). Retrieved November 22, 2013.
21. "The Many Lives of Herbert O. Yardley" ([https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/many\\_lives.pdf](https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/many_lives.pdf)) (PDF). Retrieved May 26, 2016.

22. Yardley, Herbert O. (1931). *The American black chamber*. Annapolis, MD: Naval Institute Press. ISBN 978-1-59114-989-7.
23. James Bamford. "Building America's secret surveillance state" (<http://blogs.reuters.com/great-debate/2013/06/10/building-americas-secret-surveillance-state/>). *Reuters*. Retrieved November 9, 2013.
24. Hastedt, Glenn P.; Guerrier, Steven W. (2009). *Spies, wiretaps, and secret operations: An encyclopedia of American espionage*. ABC-CLIO. p. 32. ISBN 978-1-85109-807-1.
25. USAICoE History Office. "Army Security Agency Established, 15 September 1945" (<https://www.army.mil/article/110544/>). *army.mil*. United States Army. Archived (<https://web.archive.org/web/20200716133448/https://www.army.mil/article/110544/>) from the original on July 16, 2020. Retrieved November 9, 2013.
26. Burns, Thomas L. "The Origins of the National Security Agency 1940–1952 (U)" (<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB278/02.PDF>) (PDF). *gwu.edu*. National Security Agency. p. 60. Archived (<https://web.archive.org/web/20201129024035/https://nsarchive2.gwu.edu/NSAEBB/NSAEBB278/02.PDF>) (PDF) from the original on November 29, 2020. Retrieved November 28, 2020.
27. "The Creation of NSA – Part 2 of 3: The Brownell Committee" ([https://web.archive.org/web/20130918015612/http://www.nsa.gov/public\\_info/files/crypto\\_almanac\\_50th/The\\_Creation\\_of\\_NSA\\_Part\\_3.pdf](https://web.archive.org/web/20130918015612/http://www.nsa.gov/public_info/files/crypto_almanac_50th/The_Creation_of_NSA_Part_3.pdf)) (PDF). *nsa.gov*. National Security Agency. Archived from the original ([https://www.nsa.gov/public\\_info/files/crypto\\_almanac\\_50th/The\\_Creation\\_of\\_NSA\\_Part\\_3.pdf](https://www.nsa.gov/public_info/files/crypto_almanac_50th/The_Creation_of_NSA_Part_3.pdf)) (PDF) on September 18, 2013. Retrieved July 2, 2013.
28. Truman, Harry S. (October 24, 1952). "Memorandum" ([https://web.archive.org/web/20130821073605/http://www.nsa.gov/public\\_info/files/truman/truman\\_memo.pdf](https://web.archive.org/web/20130821073605/http://www.nsa.gov/public_info/files/truman/truman_memo.pdf)) (PDF). *nsa.gov*. National Security Agency. Archived from the original ([https://www.nsa.gov/public\\_info/files/truman/truman\\_memo.pdf](https://www.nsa.gov/public_info/files/truman/truman_memo.pdf)) (PDF) on August 21, 2013. Retrieved July 2, 2013.
29. Burns, Thomas L. (1990). "The Origins of the National Security Agency" ([https://web.archive.org/web/20160322122158/https://www.nsa.gov/public\\_info/files/cryptologic\\_histories/origins\\_of\\_nsa.pdf](https://web.archive.org/web/20160322122158/https://www.nsa.gov/public_info/files/cryptologic_histories/origins_of_nsa.pdf)) (PDF). United States Cryptologic History. National Security Agency. pp. 107–08. Archived from the original ([https://www.nsa.gov/public\\_info/files/cryptologic\\_histories/origins\\_of\\_nsa.pdf](https://www.nsa.gov/public_info/files/cryptologic_histories/origins_of_nsa.pdf)) (PDF) on March 22, 2016.
30. Anne Gearan (June 7, 2013). "'No Such Agency' spies on the communications of the world" ([https://www.washingtonpost.com/world/national-security/no-such-agency-spies-on-the-communications-of-the-world/2013/06/06/5bcd46a6-ceb9-11e2-8845-d970ccb04497\\_story.html](https://www.washingtonpost.com/world/national-security/no-such-agency-spies-on-the-communications-of-the-world/2013/06/06/5bcd46a6-ceb9-11e2-8845-d970ccb04497_story.html)). *The Washington Post*. Retrieved November 9, 2013.
31. Shane, Scott (October 31, 2005). "Vietnam Study, Casting Doubts, Remains Secret" (<https://www.nytimes.com/2005/10/31/politics/31war.html>). *The New York Times*. "The National Security Agency has kept secret since 2001 a finding by an agency historian that during the Tonkin Gulf episode, which helped precipitate the Vietnam War"
32. "Declassified NSA Files Show Agency Spied on Muhammad Ali and MLK Operation Minaret Set Up in the 1960s to Monitor Anti-Vietnam Critics, Branded 'Disreputable If Not Outright Illegal' by NSA Itself" (<https://www.theguardian.com/world/2013/sep/26/nsa-surveillance-anti-vietnam-muhammad-ali-mlk>) *The Guardian*, September 26, 2013
33. Boak, David G. (July 1973) [1966]. *A History of U.S. Communications Security; the David G. Boak Lectures, Vol. 1* ([https://www.governmentattic.org/18docs/Hist\\_US\\_COMSEC\\_Boak\\_NS\\_A\\_1973u.pdf](https://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NS_A_1973u.pdf)) (PDF) (2015 partial declassification ed.). Ft. George G. Meade, MD: U.S. National Security Agency. Retrieved 2017-04-23.
34. "Pre-Emption – The Nsa And The Telecoms – Spying On The Home Front – FRONTLINE – PBS" (<https://www.pbs.org/wgbh/pages/frontline/homefront/preemption/telecoms.html>). *pbs.org*.
35. Cohen, Martin (2006). *No Holiday: 80 Places You Don't Want to Visit* ([https://books.google.com/books?id=Pj1\\_-1a79kkC&q=9781932857290](https://books.google.com/books?id=Pj1_-1a79kkC&q=9781932857290)). New York: Disinformation Company Ltd. ISBN 978-1-932857-29-0. Retrieved March 14, 2014.

36. William Burr, ed. (September 25, 2017). "National Security Agency Tracking of U.S. Citizens – "Questionable Practices" from 1960s & 1970s" (<https://nsarchive.gwu.edu/briefing-book/cyber-audit-intelligence-nuclear-vault/2017-09-25/national-security-agency-tracking-us>). National Security Archive. Retrieved August 2, 2018.
37. Bill Moyers Journal (October 26, 2007). "The Church Committee and FISA" (<https://www.pbs.org/moyers/journal/10262007/profile2.html>). Public Affairs Television. Retrieved June 28, 2013.
38. "Book IV, Supplementary Detailed Staff Reports on Foreign and Military Intelligence (94th Congress, Senate report 94-755)" ([https://web.archive.org/web/20130922044847/http://www.intelligence.senate.gov/pdfs94th/94755\\_IV.pdf](https://web.archive.org/web/20130922044847/http://www.intelligence.senate.gov/pdfs94th/94755_IV.pdf)) (PDF). United States Senate Select Committee on Intelligence. April 23, 1976. p. 67 (72). Archived from the original ([http://www.intelligence.senate.gov/pdfs94th/94755\\_IV.pdf](http://www.intelligence.senate.gov/pdfs94th/94755_IV.pdf)) (PDF) on September 22, 2013. Retrieved June 28, 2013.
39. "Book II, Intelligence Activities and the Rights of Americans (94th Congress, Senate report 94-755)" ([https://web.archive.org/web/20130521200703/https://www.intelligence.senate.gov/pdfs94th/94755\\_II.pdf](https://web.archive.org/web/20130521200703/https://www.intelligence.senate.gov/pdfs94th/94755_II.pdf)) (PDF). United States Senate Select Committee on Intelligence. April 26, 1976. p. 124 (108). Archived from the original ([http://www.intelligence.senate.gov/pdfs94th/94755\\_II.pdf](http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf)) (PDF) on May 21, 2013. Retrieved June 28, 2013.
40. Seymour M. Hersh (February 22, 1987). "Target Qaddafi" (<https://www.nytimes.com/1987/02/22/magazine/target-qaddafi.html?pagewanted=all>). *The New York Times*. Retrieved January 12, 2014.
41. David Wise (May 18, 1986). "Espionage Case Pits CIA Against News Media" ([http://articles.latimes.com/1986-05-18/opinion/op-21101\\_1\\_news-media2](http://articles.latimes.com/1986-05-18/opinion/op-21101_1_news-media2)). *The Los Angeles Times*. Retrieved January 12, 2014. "the President took an unprecedented step in discussing the content of the Libyan cables. He was, by implication, revealing that NSA had broken the Libyan code."
42. Peggy Becker (October 1999). Development of Surveillance Technology and Risk of Abuse of Economic Information (<http://www.europarl.europa.eu/stoa/cms/cache/offonce/home/publications/studies?page=12>) (Report). STOA, European Parliament. p. 12. Retrieved November 3, 2013.
43. Staff (June 13, 2003). "NSA honors 4 in the science of codes" ([http://articles.baltimoresun.com/2003-06-13/news/0306130156\\_1\\_cryptology-hall-of-honor-pioneers](http://articles.baltimoresun.com/2003-06-13/news/0306130156_1_cryptology-hall-of-honor-pioneers)). *The Baltimore Sun*. Tribune Company. Retrieved June 11, 2013.
44. James Bamford (2007). *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* (<https://books.google.com/books?id=VqY4Wr3T5K4C&pg=PA454>). Knopf Doubleday Publishing Group. p. 454. ISBN 978-0-307-42505-8.
45. Koblit, Neal (2008). *Random Curves: Journeys of a Mathematician*. Springer-Verlag. p. 312. ISBN 9783540740773.
46. Landau, Susan (2015), "NSA and Dual EC\_DRBG: Deja vu all over again?", *The Mathematical Intelligencer*, **37** (4): 72–83, doi:10.1007/s00283-015-9543-z (<https://doi.org/10.1007/s00283-015-9543-z>), S2CID 124392006 (<https://api.semanticscholar.org/CorpusID:124392006>)
47. Curtis, Sophie (13 November 2014). "Ex-NSA technical chief: How 9/11 created the surveillance state" (<https://www.telegraph.co.uk/technology/internet-security/11221287/Ex-NSA-technical-chief-How-911-created-the-surveillance-state.html>). *The Daily Telegraph*.
48. "In 2002 Brian Snow was moved from the technical directorship of IAD to a different position within the NSA that had high status but little influence, particularly with regard to actions that were being proposed by SIGINT; Mike Jacobs retired from the NSA the same year." Koblit, Neal; Menezes, Alfred J. (2016), "A riddle wrapped in an enigma", *IEEE Security & Privacy*, **14** (6): 34–42, doi:10.1109/MSP.2016.120 (<https://doi.org/10.1109/MSP.2016.120>), S2CID 2310733 (<https://api.semanticscholar.org/CorpusID:2310733>) Footnote 9 in the full version, see "A riddle wrapped in an enigma" (<https://eprint.iacr.org/2015/1018.pdf>) (PDF). Retrieved 12 April 2018.

49. Gorman, Siobhan (May 17, 2006). "NSA killed system that sifted phone data legally" (<https://web.archive.org/web/20070927193047/http://www.baltimoresun.com/news/nationworld/bal-te.nsa18may18%2C1%2C5386811.story?ctrack=1&cset=true>). *Baltimore Sun*. Tribune Company (Chicago, IL). Archived from the original (<http://www.baltimoresun.com/news/nationworld/bal-te.nsa18may18,1,5386811.story>) on September 27, 2007. Retrieved March 7, 2008. "The privacy protections offered by ThinThread were also abandoned in the post–September 11 push by the president for a faster response to terrorism."
50. Bamford, *Shadow Factory*, pp. 325–340.
51. Baltimore Sun (May 6, 2007). "Management shortcomings seen at NSA" (<http://www.baltimoresun.com/news/nation-world/bal-nsa050607,0,1517618.story>). *baltimoresun.com*.
52. "NSA surveillance exposed by Snowden ruled unlawful" (<https://www.bbc.com/news/technology-54013527>). *BBC*. Retrieved 4 September 2020.
53. Bamford, James (December 25, 2005). "The Agency That Could Be Big Brother" (<https://www.nytimes.com/2005/12/25/weekinreview/25bamford.html>). *The New York Times*. Retrieved September 11, 2005.
54. Dana Priest, William Arkin (July 19, 2010). "A hidden world, growing beyond control]" (<http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print/>). *The Washington Post*.
55. "National Security Agency and the U.S. Department of Homeland Security Form New Partnership to Increase National Focus on Cyber Security Education" ([https://web.archive.org/web/20090117020321/http://www.nsa.gov/public\\_info/press\\_room/2004/nsa\\_dhs\\_new\\_partnership.shtml](https://web.archive.org/web/20090117020321/http://www.nsa.gov/public_info/press_room/2004/nsa_dhs_new_partnership.shtml)) (Press release). NSA Public and Media Affairs. April 22, 2004. Archived from the original ([https://www.nsa.gov/public\\_info/press\\_room/2004/nsa\\_dhs\\_new\\_partnership.shtml](https://www.nsa.gov/public_info/press_room/2004/nsa_dhs_new_partnership.shtml)) on 2009-01-17. Retrieved July 4, 2008.
56. Hager, Nicky (1996). *Secret Power: New Zealand's Role in the International Spy Network*. Craig Potton Publishing. p. 55. ISBN 978-0-908802-35-7.
57. "It's kind of a legacy system, this whole idea, the Echelon," Bamford said. "Communications have changed a great deal since they built it." in Muir, Pat (May 27, 2013). "Secret Yakima facility may be outdated, expert says" (<https://archive.today/20130616081534/http://www.yakimaherald.com/news/latestpoliticsnews/1142385-8/new-details-on-the-nsas-closure-of-its>). *Yakima Herald-Republic*. Seattle Times. Archived from the original (<http://www.yakimaherald.com/news/latestpoliticsnews/1142385-8/new-details-on-the-nsas-closure-of-its>) on June 16, 2013. Retrieved June 15, 2013.
58. Richelson, Jeffrey T.; Ball, Desmond (1985). *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*. London: Allen & Unwin. ISBN 0-04-327092-1
59. Patrick S. Poole, Echelon: America's Secret Global Surveillance Network (Washington, D.C.: Free Congress Foundation, October 1998)
60. Echelon" (<http://www.cbsnews.com/news/ex-snoop-confirms-echelon-network/>), *60 Minutes*, February 27, 2000
61. Campbell, Duncan (August 12, 1988). "They've Got It Taped" (<https://web.archive.org/web/20130614020755/http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf>) (PDF). *New Statesman via duncancampbell.org*. Archived from the original (<http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf>) (PDF) on June 14, 2013. Retrieved June 19, 2007.
62. Bomford, Andrew (November 3, 1999). "Echelon spy network revealed" (<http://news.bbc.co.uk/2/hi/503224.stm>). BBC. Retrieved June 7, 2013.
63. "European Parliament Report on Echelon" ([https://fas.org/irp/program/process/rapport\\_echelon\\_en.pdf](https://fas.org/irp/program/process/rapport_echelon_en.pdf)) (PDF). July 2001. Retrieved July 4, 2008.

64. Glenn Greenwald (November 26, 2013). "Top-Secret Documents Reveal NSA Spied on Porn Habits as Part of Plan to Discredit 'Radicalizers'" ([http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims\\_n\\_4346128.html?1385526024](http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html?1385526024)). *The Huffington Post*. London. Retrieved May 6, 2014.
65. James Risen; Laura Poitras (May 31, 2014). "N.S.A. Collecting Millions of Faces From Web Images" (<https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html>). *The New York Times*. Retrieved June 1, 2014.
66. Ellen Nakashima; Joby Warrick (July 14, 2013). "For NSA chief, terrorist threat drives passion to 'collect it all,' observers say" ([https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211\\_story.html](https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html)). *The Washington Post*. Retrieved July 15, 2013. "Collect it all, tag it, store it. . . . And whatever it is you want, you go searching for it."
67. Glenn Greenwald (July 15, 2013). "The crux of the NSA story in one phrase: 'collect it all': The actual story that matters is not hard to see: the NSA is attempting to collect, monitor and store all forms of human communication" (<https://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all>). *The Guardian*. Retrieved July 16, 2013.
68. Greg Miller and Julie Tate, October 17, 2013, "Documents reveal NSA's extensive involvement in targeted killing program" ([https://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc\\_story.html](https://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html)), *The Washington Post*. Retrieved October 18, 2013.
69. Laura Poitras, Marcel Rosenbach, Fidelius Schmid und Holger Stark. "Geheimdokumente: NSA horcht EU-Vertretungen mit Wanzen aus (<http://www.spiegel.de/netzwelt/netzpolitik/nsa-hat-wanzen-in-eu-gebaeuden-installiert-a-908515.html>)". *Der Spiegel* (in German). Retrieved June 29, 2013.
70. "US-Geheimdienst hörte Zentrale der Vereinten Nationen ab (<http://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html>)". *Der Spiegel* (in German). Retrieved August 25, 2013.
71. Spiegel.de: Wikileaks-Enthüllung, NSA soll auch französische Wirtschaft bespitzelt haben (German) (<http://www.spiegel.de/politik/ausland/wikileaks-enthuellung-nsa-soll-auch-franzoesische-wirtschaft-bespitzelt-haben-a-1041268.html>), June 2015
72. kwi (July 9, 2015). "Wikileaks: Und täglich grüßt die NSA" (<https://www.handelsblatt.com/politik/deutschland/wikileaks-und-taeglich-gruesst-die-nsa/12034888.html>). *handelsblatt.com*.
73. Sueddeutsche.de: US-Spionage ist eine Demütigung für Deutschland (German) (<http://www.sueddeutsche.de/politik/nsa-skanal-us-spionage-ist-eine-demuetigung-fuer-deutschland-1.2558131>), 10 July 2015
74. "NSA tapped German Chancellery for decades, WikiLeaks claims" (<https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel>). *The Guardian*. Reuters. 8 July 2015.
75. France in the NSA's crosshair : phone networks under surveillance ([http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance\\_3499741\\_651865.html](http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html)) Le Monde October 21, 2013
76. Perlroth, Nicole (September 10, 2013). "Government Announces Steps to Restore Confidence on Encryption Standards" (<http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/>). *The New York Times* (Bits blog).
77. Perlroth, Nicole, Larson, Jeff, and Shane, Scott (September 5, 2013). "The NSA's Secret Campaign to Crack, Undermine Internet Security" (<https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>). ProPublica. "This story has been reported in partnership between The New York Times, the Guardian and ProPublica based on documents obtained by The Guardian. For the Guardian: James Ball, Julian Borger, Glenn Greenwald; For the New York Times: Nicole Perlroth, Scott Shane; For ProPublica: Jeff Larson"

78. "Schneier on Security: The Strange Story of Dual\_EC\_DRBG" ([https://www.schneier.com/blog/archives/2007/11/the\\_strange\\_sto.html](https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html)). Schneier.com. November 15, 2007. Retrieved October 9, 2013.
79. J. Appelbaum; A. Gibson; J. Goetz; V. Kabisch; L. Kampf; L. Ryge (July 3, 2014). "NSA targets the privacy-conscious" ([http://daserste.ndr.de/panorama/aktuell/nsa230\\_page-1.html](http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html)). *Panorama*. Norddeutscher Rundfunk. Retrieved July 4, 2014.
80. Lena Kampf, Jacob Appelbaum & John Goetz, Norddeutscher Rundfunk (July 3, 2014). "Deutsche im Visier des US-Geheimdienstes: Von der NSA als Extremist gebrandmarkt" (<http://www.tagesschau.de/inland/nsa-xkeyscore-100.html>) (in German). *ARD*.
81. "TechWeekEurope: Linus Torvalds Jokes The NSA Wanted A Backdoor In Linux" (<https://web.archive.org/web/20150916142701/http://www.linuxfoundation.org/news-media/news/2013/09/techweekeurope-linus-torvalds-jokes-nsa-wanted-backdoor-linux>). *linuxfoundation.org*. Archived from the original (<http://www.linuxfoundation.org/news-media/news/2013/09/techweekeurope-linus-torvalds-jokes-nsa-wanted-backdoor-linux>) on 2015-09-16.
82. "NSA Asked Linus Torvalds To Install Backdoors Into GNU/Linux" (<http://falkvinge.net/2013/11/17/nsa-asked-linus-torvalds-to-install-backdoors-into-gnulinux/>). *falkvinge.net*.
83. "Civil Liberties, Justice and Home Affairs – Hearings" (<http://www.europarl.europa.eu/committees/en/libe/events.html>). *europa.eu*.
84. "The Swedes discover Lotus Notes has key escrow!" *The Risks Digest*, Volume 19, Issue 52, December 24, 1997
85. *Only NSA can listen, so that's OK* Heise, 1999.
86. Gallagher, Sean (May 14, 2014). "Photos of an NSA "upgrade" factory show Cisco router getting implant" (<https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/>). *Ars Technica*.
87. Whitwam, Ryan (December 30, 2013). "The NSA regularly intercepts laptop shipments to implant malware report says" (<http://www.extremetech.com/computing/173721-the-nsa-regularly-intercepts-laptop-shipments-to-implant-malware-report-says/>). *extremetech.com*.
88. [http://www.spiegel.de/static/happ/netzwelt/2014/na/v1/pub/img/USB/S3223\\_COTTONMOUTH-l.jpg](http://www.spiegel.de/static/happ/netzwelt/2014/na/v1/pub/img/USB/S3223_COTTONMOUTH-l.jpg)
89. nsa.gov: The NSA story ([https://www.nsa.gov/public\\_info/files/speeches\\_testimonies/2013\\_08\\_09\\_the\\_nsa\\_story.pdf](https://www.nsa.gov/public_info/files/speeches_testimonies/2013_08_09_the_nsa_story.pdf)) Archived ([https://web.archive.org/web/20141209113543/https://www.nsa.gov/public\\_info/files/speeches\\_testimonies/2013\\_08\\_09\\_the\\_nsa\\_story.pdf](https://web.archive.org/web/20141209113543/https://www.nsa.gov/public_info/files/speeches_testimonies/2013_08_09_the_nsa_story.pdf)) 2014-12-09 at the *Wayback Machine*, retrieved January 19, 2015 – Page 3: 'NSA ... will work with the FBI and other agencies to connect the dots between foreign-based actors and their activities in the U.S.'
90. Domestic Surveillance Directorate website (<https://nsa.gov1.info/>), retrieved January 19, 2015
91. *forbes.com*: The Definitive NSA Parody Site Is Actually Informative (<https://www.forbes.com/sites/kashmirhill/2013/08/29/the-definitive-nsa-parody-site-is-actually-informative/>), retrieved January 19, 2015
92. John D Bates (October 3, 2011). "[redacted]" ([https://www.eff.org/sites/default/files/filenode/fisc\\_opinion\\_-\\_unconstitutional\\_surveillance\\_0.pdf](https://www.eff.org/sites/default/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf)) (PDF). pp. 73–74.
93. David Alan Jordan. Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice over Internet Protocol ([http://iilj.org/documents/Jordan-47\\_BC\\_L\\_Rev\\_000.pdf](http://iilj.org/documents/Jordan-47_BC_L_Rev_000.pdf)) Archived ([https://web.archive.org/web/20071030095250/http://www.ss8.com/pdfs/Ready\\_Guide\\_Download\\_Version.pdf](https://web.archive.org/web/20071030095250/http://www.ss8.com/pdfs/Ready_Guide_Download_Version.pdf)) 2007-10-30 at the *Wayback Machine*. *Boston College Law Review*. May 2006. Last access date January 23, 2007
94. Provost, Colin (2009). *President George W. Bush's Influence Over Bureaucracy and Policy* (<https://archive.org/details/presidentgeorgew0000unse/page/94>). Palgrave Macmillan. pp. 94–99 (<https://archive.org/details/presidentgeorgew0000unse/page/94>). ISBN 978-0-230-60954-9.

95. Charlie Savage (2015-09-20). "George W. Bush Made Retroactive N.S.A. 'Fix' After Hospital Room Showdown" ([https://www.nytimes.com/2015/09/21/us/politics/george-w-bush-made-retroactive-nsa-fix-after-hospital-room-showdown.html?\\_r=1](https://www.nytimes.com/2015/09/21/us/politics/george-w-bush-made-retroactive-nsa-fix-after-hospital-room-showdown.html?_r=1)). *The New York Times*.
96. Gellman, Barton; Poitras, Laura (June 7, 2013). "U.S. intelligence mining data from nine U.S. Internet companies in broad secret program" ([https://www.washingtonpost.com/investigations/u-s-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story.html?hpid=z1](https://www.washingtonpost.com/investigations/u-s-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1)). *The Washington Post*. Retrieved June 6, 2013.
97. Greenwald, Glenn (June 6, 2013). "NSA taps in to internet giants' systems to mine user data, secret files reveal" (<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>). *The Guardian*. London. Retrieved June 6, 2013.
98. "Microsoft handed the NSA access to encrypted messages" (<https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data>). *The Guardian*. July 12, 2013. Retrieved September 7, 2013.
99. Angwin, Julia (2014). *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance* (<https://archive.org/details/dragnetnationque0000angw>). Times Books / Henry Holt and Company. p. 47 (<https://archive.org/details/dragnetnationque0000angw/page/47>). ISBN 978-0-8050-9807-5.
00. Elliott, Justin and Meyer, Theodor *ProPublica*. Retrieved October 7, 2016. (<https://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence>)
01. "Goldman, Adam and Apuzzo, Matt Associated Press. Retrieved October 7, 2016" (<http://bigstory.ap.org/article/nyc-bomb-plot-details-settle-little-nsa-debate>).
02. "NSA program stopped no terror attacks, says White House panel member" (<https://www.nbcnews.com/news/world/nsa-program-stopped-no-terror-attacks-says-white-house-panel-flna2D11783588>). *NBC News*.
03. Masnick, Mike (December 23, 2013). "Judge And Intelligence Task Force Both Seem Stunned By Lack Of Evidence That Bulk Phone Collection Program Stops Terrorists" (<https://web.archive.org/web/20161010010635/https://www.techdirt.com/articles/20131220/11312025653/judge-in-intelligence-task-force-both-seem-stunned-nsa-couldnt-provide-single-example-data-collection-stopping-terrorism.shtml>). *Techdirt*. Archived from the original (<https://www.techdirt.com/articles/20131220/11312025653/judge-intelligence-task-force-both-seem-stunned-nsa-couldnt-provide-single-example-data-collection-stopping-terrorism.shtml>) on October 10, 2016. Retrieved 2017-10-10.
04. Aid, Matthew M. (10 June 2013). "Inside the NSA's Ultra-Secret China Hacking Group" (<https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/>). *Foreign Policy*. Retrieved 11 June 2013.
05. "U.S. NSA Unit 'TAO' Hacking China For Years (<http://www.businessinsider.com/us-nsa-unit-tao-hacking-china-for-years-2013-6>)". Business Insider. June 11, 2013
06. "Secret NSA hackers from TAO Office have been pwning China for nearly 15 years (<http://www.computerworld.com/article/2473609/cybercrime-hacking/secret-nsa-hackers-from-tao-office-have-been-pwning-china-for-nearly-15-years.html>)". *Computerworld*. June 11, 2013.
07. "Flubbed NSA Hack Caused Massive 2012 Syrian Internet Blackout, Snowden Says (<http://www.ibtimes.com/flubbed-nsa-hack-caused-massive-2012-syrian-internet-blackout-snowden-says-1657886>)". *International Business Times*. August 13, 2013.
08. These offices are for example mentioned in a FISA court order ([http://www.dni.gov/files/documents/PrimaryOrder\\_Collection\\_215.pdf](http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf)) from 2011.
09. "National Security Agency" (<https://fas.org/irp/nsa/oldind.html>). fas.org. Retrieved October 9, 2013.
10. Matthew M. Aid, *The Secret Sentry*, New York, 2009, pp. 130, 138, 156–158.
11. See also the information about the historical structure of NSA that is archived at FAS.org (<https://fas.org/irp/nsa/oldind.html#organizations>)

12. TheWeek.com: The NSA's secret org chart (<http://theweek.com/article/index/249658/the-nsas-secret-org-chart>), September 15, 2013
13. National Security Agency – 60 Years of Defending Our Nation ([https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) Archived ([https://web.archive.org/web/20180623141614/https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20180623141614/https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) 2018-06-23 at the Wayback Machine, Anniversary booklet, 2012, p. 96.
14. Marc Ambinder, 3008 Selectors (<http://theweek.com/article/index/246277/3008-selectors>), June 27, 2013.
15. Ellen Nakashima. National Security Agency plans major reorganization ([https://www.washingtonpost.com/world/national-security/national-security-agency-plans-major-reorganization/2016/02/02/2a66555e-c960-11e5-a7b2-5a2f824b02c9\\_story.html](https://www.washingtonpost.com/world/national-security/national-security-agency-plans-major-reorganization/2016/02/02/2a66555e-c960-11e5-a7b2-5a2f824b02c9_story.html)). *The Washington Post*, Feb 2016.
16. National Security Agency (2009). "ARC Registration" ([https://web.archive.org/web/20120118224340/https://www.nsaarc.net/docs/arc\\_registration\\_guide.pdf](https://web.archive.org/web/20120118224340/https://www.nsaarc.net/docs/arc_registration_guide.pdf)) (PDF). NSA ARC. Archived from the original ([https://www.nsaarc.net/docs/arc\\_registration\\_guide.pdf](https://www.nsaarc.net/docs/arc_registration_guide.pdf)) (PDF) on January 18, 2012. Retrieved April 13, 2011.
17. DNI (2009). "2009 National Intelligence Consumer's Guide" ([https://web.archive.org/web/20120524093812/http://www.dni.gov/reports/IC\\_Consumers\\_Guide\\_2009.pdf](https://web.archive.org/web/20120524093812/http://www.dni.gov/reports/IC_Consumers_Guide_2009.pdf)) (PDF). Director of National Intelligence. Archived from the original ([http://www.dni.gov/reports/IC\\_Consumers\\_Guide\\_2009.pdf](http://www.dni.gov/reports/IC_Consumers_Guide_2009.pdf)) (PDF) on May 24, 2012. Retrieved April 13, 2011.
18. US Army. "Theater Army Operations, Field Manual No. 3-93 (100–7)" ([https://web.archive.org/web/20110824235523/http://portal.dean.usma.edu/departments/se/nrcd/PDFs/FM%203-93%20\(Final%20Draft,%20Jul%2010\).pdf](https://web.archive.org/web/20110824235523/http://portal.dean.usma.edu/departments/se/nrcd/PDFs/FM%203-93%20(Final%20Draft,%20Jul%2010).pdf)) (PDF). Archived from the original ([http://portal.dean.usma.edu/departments/se/nrcd/PDFs/FM%203-93%20\(Final%20Draft,%20Jul%2010\).pdf](http://portal.dean.usma.edu/departments/se/nrcd/PDFs/FM%203-93%20(Final%20Draft,%20Jul%2010).pdf)) (PDF) on August 24, 2011. Retrieved April 13, 2011.
19. Lackland Security Hill Enterprise Infrastructure and Computer Systems Management (<http://static.e-publishing.af.mil/production/1/67nww/publication/67nwwi33-1160/67nwwi33-1160.pdf>) Archived (<https://web.archive.org/web/20140204013239/http://static.e-publishing.af.mil/production/1/67nww/publication/67nwwi33-1160/67nwwi33-1160.pdf>) 2014-02-04 at the Wayback Machine, October 1, 2010, p. 2.
20. Marc Ambinder, How a single IT tech could spy on the world (<http://theweek.com/article/index/245408/how-a-single-it-tech-could-spy-on-the-world>), June 10, 2013.
21. Misiewicz (September 1998). "Thesis; Modeling and Simulation of a Global Reachback Architecture ..." ([https://web.archive.org/web/20110812153842/http://edocs.nps.edu/npspubs/scholarly/theses/1998/Sep/98Sep\\_Misiewicz.pdf](https://web.archive.org/web/20110812153842/http://edocs.nps.edu/npspubs/scholarly/theses/1998/Sep/98Sep_Misiewicz.pdf)) (PDF). Archived from the original ([http://edocs.nps.edu/npspubs/scholarly/theses/1998/Sep/98Sep\\_Misiewicz.pdf](http://edocs.nps.edu/npspubs/scholarly/theses/1998/Sep/98Sep_Misiewicz.pdf)) (PDF) on August 12, 2011. Retrieved April 13, 2011.
22. Joe Jarzombek (2004). "Systems, Network, and Information Integration Context for Software Assurance" (<http://www.sei.cmu.edu/library/assets/jarzombek.pdf>) (PDF). Carnegie Mellon University. Retrieved April 13, 2011.
23. Christopher Griffin (2010). "Dealing with Sensitive Data at Penn State's Applied Research Laboratory: Approach and Examples" ([http://www.exportcontrols.msu.edu/FBI\\_2010/Dr\\_Christopher\\_Griffin\\_Applied\\_Research\\_Laboratories\\_Penn\\_State\\_University\\_10\\_20\\_2010.pdf](http://www.exportcontrols.msu.edu/FBI_2010/Dr_Christopher_Griffin_Applied_Research_Laboratories_Penn_State_University_10_20_2010.pdf)) (PDF). msu.edu. Retrieved April 13, 2011.
24. NPR.org: Officials: Edward Snowden's Leaks Were Masked By Job Duties (<https://www.npr.org/2013/09/18/223523622/officials-edward-snowdens-leaks-were-masked-by-job-duties>), September 18, 2013.
25. Top Level Telecommunications: Pictures at the NSA's 60th anniversary (<http://electrospace.blogspot.com/2012/12/pictures-at-nsas-60th-anniversary.html>)
26. National Security Agency – 60 Years of Defending Our Nation ([https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) Archived ([https://web.archive.org/web/20180623141614/https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20180623141614/https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) 2018-06-23 at the Wayback Machine, Anniversary booklet, 2012, p. 102.

27. Matthew M. Aid, *The Secret Sentry*, New York, 2009, pp. 128, 148, 190 and 198.
28. Harvey A. Davis (March 12, 2002). *Statement for the Record* ([https://web.archive.org/web/20090619013425/http://www.nsa.gov/public\\_info/speeches\\_testimonies/12mar02.shtml](https://web.archive.org/web/20090619013425/http://www.nsa.gov/public_info/speeches_testimonies/12mar02.shtml)) (Speech). 342 Dirksen Senate Office Building, Washington, D.C. Archived from the original ([https://www.nsa.gov/public\\_info/speeches\\_testimonies/12mar02.shtml](https://www.nsa.gov/public_info/speeches_testimonies/12mar02.shtml)) on June 19, 2009. Retrieved November 24, 2009.
29. Drew, Christopher & Somini Sengupta (June 24, 2013). "N.S.A. Leak Puts Focus on System Administrators" (<https://www.nytimes.com/2013/06/24/technology/nsa-leak-puts-focus-on-system-administrators.html>). *The New York Times*. Retrieved June 25, 2013.
30. David Kahn, *The Codebreakers*, Scribner Press, 1967, chapter 19, pp. 672–733.
31. Barton Gellman (December 25, 2013). "Edward Snowden, after months of NSA revelations, says his mission's accomplished" ([https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d\\_story.html](https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html)). *The Washington Post*.
32. Bauer, Craig P. (2013). *Secret History: The Story of Cryptology* (<https://books.google.com/books?id=EBkEGAOICDsC&pg=PA359>). CRC Press. p. 359. ISBN 978-1-4665-6186-1.
33. Bamford (18 December 2007). "page 538" (<https://books.google.com/books?id=VqY4Wr3T5K4C&pg=PA538>). *Body of Secrets*. ISBN 9780307425058.
34. "Your Polygraph Examination: An Important Appointment to Keep" ([https://web.archive.org/web/20130903162514/http://www.nsa.gov/careers/\\_files/poly\\_brochure\\_final2.pdf](https://web.archive.org/web/20130903162514/http://www.nsa.gov/careers/_files/poly_brochure_final2.pdf)) (PDF). National Security Agency. Archived from the original ([https://www.nsa.gov/careers/\\_files/poly\\_brochure\\_final2.pdf](https://www.nsa.gov/careers/_files/poly_brochure_final2.pdf)) (PDF) on 2013-09-03. Retrieved June 17, 2013.
35. McCarthy, Susan. "The truth about the polygraph" (<http://www.salon.com/2000/03/02/polygraph/>). *Salon*. Retrieved July 5, 2013.
36. Nagesh, Gautham (June 14, 2010). "NSA video tries to dispel fear about polygraph use during job interviews" (<http://thehill.com/blogs/hillicon-valley/technology/102963-nsa-video-comes-clean-on-polygraph-use>). *The Hill*. Retrieved June 15, 2013.
37. Stein, Jeff. "NSA lie detectors no sweat, video says ([http://voices.washingtonpost.com/spy-talk/2010/06/facing\\_nsas\\_lie\\_detector\\_relax.html](http://voices.washingtonpost.com/spy-talk/2010/06/facing_nsas_lie_detector_relax.html))." *The Washington Post*. June 14, 2010. Retrieved July 5, 2013.
38. Maschke, George (13 June 2010). "The Truth About the Polygraph (According to the NSA)" ([https://www.youtube.com/watch?v=93\\_FDeMENN4](https://www.youtube.com/watch?v=93_FDeMENN4)). *Youtube*. Retrieved 15 July 2020.
39. Drezner, Daniel. "Tone-Deaf at the Listening Post ([https://foreignpolicy.com/articles/2013/12/16/tone\\_deaf\\_at\\_the\\_listening\\_post\\_my\\_day\\_at\\_the\\_NSA](https://foreignpolicy.com/articles/2013/12/16/tone_deaf_at_the_listening_post_my_day_at_the_NSA))." *Foreign Policy*. December 16, 2013. Retrieved March 1, 2014. "Snowden has also changed the way the NSA is doing business. Analysts have gone from being polygraphed once every five years to once every quarter."
40. "60 Years of Defending Our Nation" ([https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF). National Security Agency. 2012. p. 15. Archived from the original ([https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF) on 2013-06-14. Retrieved July 6, 2013.
41. "60 Years of Defending Our Nation" ([https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF). National Security Agency. 2012. p. 10. Archived from the original ([https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF) on 2013-06-14. Retrieved July 6, 2013.
42. "60 Years of Defending Our Nation" ([https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF). National Security Agency. 2012. p. 23. Archived from the original ([https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF) on 2013-06-14. Retrieved July 6, 2013.

43. "60 Years of Defending Our Nation" ([https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20130614022314/http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF). National Security Agency. 2012. p. 39. Archived from the original ([https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf)) (PDF) on 2013-06-14. Retrieved July 6, 2013.
44. "Marine Cryptologic Support Battalion: Intelligence Department: Fort Meade, MD: New Joins" (<http://www.hqmc.marines.mil/intelligence/Units/MarineCryptologicSupportBattalion/NewJoins.aspx>). United States Marine Corps. Retrieved June 11, 2013.
45. "Just off the Baltimore-Washington Parkway, about 25 miles northeast of Washington, is a secret city. Fort Meade, in suburban Maryland, is home to the National Security Agency – the NSA, sometimes wryly referred to as No Such Agency or Never Say Anything." and "It contains almost 70 miles of roads, 1,300 buildings, each identified by a number, and 18,000 parking spaces as well as a shopping centre, golf courses, chain restaurants and every other accoutrement of Anywhere, USA." in "Free introduction to: Who's reading your emails?" ([http://www.thesundaytimes.co.uk/sto/news/world\\_news/Americas/article1271197.ece](http://www.thesundaytimes.co.uk/sto/news/world_news/Americas/article1271197.ece)). *The Sunday Times*. June 9, 2013. Retrieved June 11, 2013.(subscription required)
46. Sernovitz, Daniel J. "NSA opens doors for local businesses (<http://www.bizjournals.com/baltimore/stories/2010/08/23/daily33.html?page=all>)." *Baltimore Business Journal*. August 26, 2010. Updated August 27, 2010. Retrieved June 11, 2013. "But for many more, the event was the first time attendees got the chance to take the "NSA Employees Only" exit off the Baltimore-Washington Parkway beyond the restricted gates of the agency's headquarters."
47. Weiland and Wilsey, p. 208 (<https://books.google.com/books?id=BywaW1f4iQ4C&pg=PA208>). "[...]housing integration has invalidated Montpelier's Ivory Pass and the National Security Agency has posted an exit ramp off the Baltimore-Washington Parkway that reads NSA."
48. Grier, Peter and Harry Bruinius. "In the end, NSA might not need to snoop so secretly (<http://www.csmonitor.com/USA/DC-Decoder/2013/0618/In-the-end-NSA-might-not-need-to-snoop-so-secretly>)." *The Christian Science Monitor*. June 18, 2013. Retrieved July 1, 2013.
49. Barnett, Mark L. (April 26, 2011). "Small Business Brief" (<https://web.archive.org/web/20130617050958/http://www.gbc.org/Committee%20pages/Small%20Business%20Brief%20April%202011.pdf>) (PDF). Office of Small Business Programs, NSA, via The Greater Baltimore Committee. p. 3. Archived from the original (<http://www.gbc.org/Committee%20pages/Small%20Business%20Brief%20April%202011.pdf>) (PDF) on June 17, 2013. Retrieved June 11, 2013.
50. Gorman, Siobhan (August 6, 2006). "NSA risking electrical overload" ([http://articles.baltimoresun.com/2006-08-06/news/0608060158\\_1\\_agency-power-surges-nsa](http://articles.baltimoresun.com/2006-08-06/news/0608060158_1_agency-power-surges-nsa)). *The Baltimore Sun*. Tribune Company. Retrieved June 10, 2013.
51. Dozier, Kimberly (June 9, 2013). "NSA claims know-how to ensure no illegal spying" (<http://bigstory.ap.org/article/nsa-finder-and-keeper-countless-us-secrets>). Associated Press. Retrieved June 12, 2013.
52. "Geeks 'R' us" ([https://web.archive.org/web/20130614020802/http://articles.baltimoresun.com/2010-01-13/news/bal-ed.cybersecurity13jan13\\_1\\_cyber-security-cyber-command-national-security-agency](https://web.archive.org/web/20130614020802/http://articles.baltimoresun.com/2010-01-13/news/bal-ed.cybersecurity13jan13_1_cyber-security-cyber-command-national-security-agency)). *The Baltimore Sun*. Tribune Company. January 13, 2010. Archived from the original ([http://articles.baltimoresun.com/2010-01-13/news/bal-ed.cybersecurity13jan13\\_1\\_cyber-security-cyber-command-national-security-agency](http://articles.baltimoresun.com/2010-01-13/news/bal-ed.cybersecurity13jan13_1_cyber-security-cyber-command-national-security-agency)) on June 14, 2013. Retrieved June 11, 2013.
53. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, p. 488 (<https://books.google.com/books?id=VqY4Wr3T5K4C&pg=PA488>). "At the heart of the invisible city is NSA's massive Headquarters/Operations Building. With more than sixty-eight acres of floor space,[...]" and "Entrance is first made through the two-story Visitor Control Center, one[...]"
54. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, p. 488 (<https://books.google.com/books?id=VqY4Wr3T5K4C&pg=PA488>)–489. "[...]one of more than 100 fixed watch posts within the secret city manned by the armed NSA police. It is here that clearances are checked and visitor badges are issued."

55. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, p. 490. "And then there is the red badge—[...]and is normally worn by people working in the "Red Corridor"—the drugstore and other concession areas[...]Those with a red badge are forbidden to go anywhere near classified information and are restricted to a few corridors and administrative areas—the bank, the barbershop, the cafeteria, the credit union, the airline and entertainment ticket counters." and "Once inside the white, pentagonal Visitor Control Center, employees are greeted by a six-foot painting of the NSA seal[...]"
56. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, p. 489. "It is here that clearances are checked and visitor badges are issued."
57. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, p. 491. "From the Visitor Control Center one enters the eleven-story, million OPS2A, the tallest building in the City. Shaped like a dark glass Rubik's Cube, the building houses much of NSA's Operations Directorate, which is responsible for processing the ocean of intercepts and prying open the complex cipher systems."
58. Bamford, James (June 12, 2013). "The Secret War" (<https://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/all/>). *Wired*. Retrieved June 12, 2013.
59. "Career Fields/Other Opportunities/NSA Police Officers section of the NSA website" ([https://www.nsa.gov/careers/career\\_fields/others.shtml](https://www.nsa.gov/careers/career_fields/others.shtml)). Nsa.gov. Retrieved October 9, 2013.
60. T.C. Carrington; Debra L.Z. Potts (September 1999). "*National Security Agency Newsletter, Protective Services-More Than Meets the Eye. An Overview of NSA's Protective Services volume XLVII, No. 9*" ([https://web.archive.org/web/20160318060528/https://www.nsa.gov/public\\_info/files/newsletters/Newsletter\\_Sept\\_1999.pdf](https://web.archive.org/web/20160318060528/https://www.nsa.gov/public_info/files/newsletters/Newsletter_Sept_1999.pdf)) (PDF). *nsa.gov*. pp. 8–10. Archived from the original ([https://www.nsa.gov/public\\_info/files/newsletters/Newsletter\\_Sept\\_1999.pdf](https://www.nsa.gov/public_info/files/newsletters/Newsletter_Sept_1999.pdf)) (PDF) on 2016-03-18.
61. "Explore NSA ([https://www.nsa.gov/careers/life\\_at\\_nsa/explore.shtml](https://www.nsa.gov/careers/life_at_nsa/explore.shtml))." (Archive ([https://web.archive.org/web/20130614022301/http://www.nsa.gov/careers/life\\_at\\_nsa/explore.shtml](https://web.archive.org/web/20130614022301/http://www.nsa.gov/careers/life_at_nsa/explore.shtml))) National Security Agency. Retrieved June 12, 2013. "Other Locations" and "Our employees live along the Colonial-era streets of Annapolis and Georgetown; in the suburban surroundings of Columbia; near the excitement of Baltimore's Inner Harbor; along rolling hills adjacent to working farms; near the shores of the Chesapeake Bay; and amid the monumental history of Washington, DC."
62. McCombs, Alan J. (2009-02-23). "Fort Meade launches commuter shuttle service" ([https://www.army.mil/article/17291/Fort\\_Meade\\_launches\\_commuter\\_shuttle\\_service](https://www.army.mil/article/17291/Fort_Meade_launches_commuter_shuttle_service)). United States Army. Retrieved 2017-06-25.
63. Sabar, Ariel (January 2, 2003). "NSA still subject to electronic failure" ([http://articles.baltimoresun.com/2003-01-02/news/0301020300\\_1\\_outages-electrical-and-computer-agency](http://articles.baltimoresun.com/2003-01-02/news/0301020300_1_outages-electrical-and-computer-agency)). and "Agency officials anticipated the problem nearly a decade ago as they looked ahead at the technology needs of the agency, sources said, but it was never made a priority, and now the agency's ability to keep its operations going is threatened." and "The NSA is Baltimore Gas & Electric's largest customer, using as much electricity as the city of Annapolis, according to James Bamford...." in Gorman, Siobhan (August 6, 2006). "NSA risking electrical overload" ([http://articles.baltimoresun.com/2006-08-06/news/0608060158\\_1\\_agency-power-surges-nsa](http://articles.baltimoresun.com/2006-08-06/news/0608060158_1_agency-power-surges-nsa)). and Gorman, Siobhan (January 26, 2007). "NSA electricity crisis gets Senate scrutiny" ([http://articles.baltimoresun.com/2007-01-26/news/0701260231\\_1\\_electricity-rockefeller-senate-intelligence-committee](http://articles.baltimoresun.com/2007-01-26/news/0701260231_1_electricity-rockefeller-senate-intelligence-committee)). and Gorman, Siobhan (June 24, 2007). "Power supply still a vexation for the NSA" ([http://articles.baltimoresun.com/2007-06-24/news/0706240110\\_1\\_national-security-agency-classified-electricity](http://articles.baltimoresun.com/2007-06-24/news/0706240110_1_national-security-agency-classified-electricity)). *The Baltimore Sun*. Tribune Company. Retrieved June 11, 2013.
64. GORMAN, SIOBHAN. "NSA risking electrical overload" (<https://web.archive.org/web/20200813231456/https://www.baltimoresun.com/news/bs-xpm-2006-08-06-0608060158-story.html>). *baltimoresun.com*. Archived from the original (<https://www.baltimoresun.com/news/bs-xpm-2006-08-06-0608060158-story.html>) on 2020-08-13. Retrieved 2018-12-23.

65. "The NSA uses about 65 to 75 megawatt-hours of electricity, The Sun reported last week. Its needs are projected to grow by 10 to 15 megawatt-hours by next fall." in Staff (January 26, 2007). "NSA electricity crisis gets Senate scrutiny" ([http://articles.baltimoresun.com/2007-01-26/news/0701260231\\_1\\_electricity-rockefeller-senate-intelligence-committee](http://articles.baltimoresun.com/2007-01-26/news/0701260231_1_electricity-rockefeller-senate-intelligence-committee)). *The Baltimore Sun*. Tribune Company. Retrieved June 11, 2013.
66. Bamford, James (March 15, 2012). "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)" ([https://www.wired.com/threatlevel/2012/03/ff\\_nsadatacenter/all/1](https://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1)). *Wired*. Condé Nast. Retrieved February 26, 2013.
67. Scott Shane and Tom Bowman (December 10, 1995). "No Such Agency Part Four – Rigging the Game" ([http://articles.baltimoresun.com/1995-12-10/news/1995344001\\_1\\_crypto-ag-nsa-headquarters-swiss](http://articles.baltimoresun.com/1995-12-10/news/1995344001_1_crypto-ag-nsa-headquarters-swiss)). *The Baltimore Sun*. Retrieved October 3, 2015.
68. Brown, Matthew Hay (May 6, 2013). "NSA plans new computing center for cyber threats" ([http://articles.baltimoresun.com/2013-05-06/news/bs-md-nsa-high-performance-computing-center-2-20130506\\_1\\_cyber-attacks-u-s-cyber-command-cyber-threats](http://articles.baltimoresun.com/2013-05-06/news/bs-md-nsa-high-performance-computing-center-2-20130506_1_cyber-attacks-u-s-cyber-command-cyber-threats)). *The Baltimore Sun*. Tribune Company. Retrieved June 11, 2013.
69. "National Security Agency: FY 2014 Military Construction, Defense-Wide" ([https://web.archive.org/web/20140125150402/http://comptroller.defense.gov/defbudget/fy2014/budget\\_justification/pdfs/07\\_Military\\_Construction/11-National\\_Security\\_Agency.pdf](https://web.archive.org/web/20140125150402/http://comptroller.defense.gov/defbudget/fy2014/budget_justification/pdfs/07_Military_Construction/11-National_Security_Agency.pdf)) (PDF). Office of the Under Secretary of Defense (Comptroller), USA.gov. pp. 3–4. Archived from the original ([http://comptroller.defense.gov/defbudget/fy2014/budget%5Fjustification/pdfs/07\\_Military\\_Construction/11-National\\_Security\\_Agency.pdf](http://comptroller.defense.gov/defbudget/fy2014/budget%5Fjustification/pdfs/07_Military_Construction/11-National_Security_Agency.pdf)) (PDF) on January 25, 2014. Retrieved June 13, 2013.
70. "The DoD Computer Security Center (DoDCSC) was established in January 1981..." and "In 1985, DoDCSC's name was changed to the National Computer Security Center..." and "its responsibility for computer security throughout the federal government..." in "A Guide to Understanding Audit in Trusted Systems" (<https://web.archive.org/web/20121106123647/http://csrc.nist.gov/publications/secpubs/rainbow/tg001.txt>). National Computer Security Center via National Institute of Standards and Technology CSRC. Archived from the original (<http://csrc.nist.gov/publications/secpubs/rainbow/tg001.txt>) on 2012-11-06. Retrieved June 30, 2013.
71. "NSA and its National Computer Security Center (NCSC) have responsibility for..." in "Computer Systems Laboratory Bulletin" (<https://web.archive.org/web/20130702193745/http://csrc.nist.gov/publications/nistbul/csl91-02.txt>). National Institute of Standards and Technology CSRC. February 1991. Archived from the original (<http://csrc.nist.gov/publications/nistbul/csl91-02.txt>) on 2013-07-02. Retrieved June 30, 2013.
72. "NSA/NCSC Rainbow Series" (<https://fas.org/irp/nsa/rainbow.htm>). Federation of American Scientists. Retrieved June 30, 2013.
73. "Fort Meade" (<https://web.archive.org/web/20130614020751/http://www.public.navy.mil/necc/ecrc/Pages/FortMeade.aspx>). Expeditionary Combat Readiness Center, United States Navy. Archived from the original (<http://www.public.navy.mil/necc/ecrc/Pages/FortMeade.aspx>) on June 14, 2013. Retrieved June 11, 2013.
74. Steve Fidel (January 6, 2011). "Utah's billion cyber-security center under way" (<http://www.deseretnews.com/article/705363940/Utahs-15-billion-cyber-security-center-under-way.html>). *Deseret News*. Retrieved January 6, 2011.
75. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (September 17, 2014). "MilCon Status Report - August, 2014 - Under Secretary of Defense for AT&L" ([https://web.archive.org/web/20141210071515/http://www.acq.osd.mil/ie/fim/library/milcon/MILCON\\_EOM-AUG\\_Report\\_2014-09-17.xlsx](https://web.archive.org/web/20141210071515/http://www.acq.osd.mil/ie/fim/library/milcon/MILCON_EOM-AUG_Report_2014-09-17.xlsx)). Archived from the original ([http://www.acq.osd.mil/ie/fim/library/milcon/MILCON\\_EOM-AUG\\_Report\\_2014-09-17.xlsx](http://www.acq.osd.mil/ie/fim/library/milcon/MILCON_EOM-AUG_Report_2014-09-17.xlsx)) on December 10, 2014. Retrieved April 16, 2015.
76. LaPlante, Matthew D. (July 2, 2009). "New NSA center unveiled in budget documents" ([http://www.sltrib.com/news/ci\\_12744661](http://www.sltrib.com/news/ci_12744661)). *The Salt Lake Tribune*. MediaNews Group. Retrieved June 9, 2013.

77. Norton-Taylor, Richard (March 1, 2012). "Menwith Hill eavesdropping base undergoes massive expansion" (<https://www.theguardian.com/world/2012/mar/01/menwith-hill-eavesdropping-base-expansion>). *The Guardian*. London: Guardian News and Media. Retrieved June 10, 2013.
78. Richelson, Jeffrey T. (August 2012). "Eavesdroppers in Disguise" (<http://www.airforcemag.com/MagazineArchive/Pages/2012/August%202012/0812Eavesdroppers.aspx>). *Air Force Magazine*. Air Force Association. Retrieved June 10, 2013.
79. Troianello, Craig (April 4, 2013). "NSA to close Yakima Training Center facility" (<https://archive.today/20130616052825/http://www.yakimaherald.com/news/latestlocalnews/1006429-8/nsa-to-close-yakima-training-center-facility>). Yakima Herald-Republic. Archived from the original (<http://www.yakimaherald.com/news/latestlocalnews/1006429-8/nsa-to-close-yakima-training-center-facility>) on June 16, 2013. Retrieved June 15, 2013.
80. "UKUSA Agreement Release: 1940–1956" ([https://web.archive.org/web/20130702172840/http://www.nsa.gov/public\\_info/declass/ukusa.shtml](https://web.archive.org/web/20130702172840/http://www.nsa.gov/public_info/declass/ukusa.shtml)). National Security Agency. Archived from the original ([https://www.nsa.gov/public\\_info/declass/ukusa.shtml](https://www.nsa.gov/public_info/declass/ukusa.shtml)) on July 2, 2013. Retrieved July 11, 2013.
81. Bamford, James (September 13, 2002). "What big ears you have" (<https://www.theguardian.com/uk/2002/sep/14/privacy>). *The Guardian*. London. Retrieved July 11, 2013.
82. Tangimoana listed in: "Government Communications Security Bureau [GCSB]" ([https://fas.org/irp/world/new\\_zealand/gcsb/index.html](https://fas.org/irp/world/new_zealand/gcsb/index.html)). Federation of American Scientists. Retrieved July 11, 2013.
83. "ECHELON Main Stations" (<https://web.archive.org/web/20131022081511/http://world-information.org/wio/infostructure/100437611746/100438659207/?ic=100446325241>). World-Information.org. Archived from the original (<http://world-information.org/wio/infostructure/100437611746/100438659207/?ic=100446325241>) on October 22, 2013. Retrieved July 11, 2013.
84. "UK agrees missile defence request" ([http://news.bbc.co.uk/1/hi/uk\\_politics/6916262.stm](http://news.bbc.co.uk/1/hi/uk_politics/6916262.stm)). *BBC News*. July 25, 2007. Retrieved June 10, 2013.
85. Campbell, Duncan (December 6, 1999). "1980 – America's big ear on Europe" (<http://www.newstatesman.com/node/136356>). *New Statesman*. Retrieved June 15, 2013.
86. Laura Poitras, Marcel Rosenbach and Holger Stark, Ally and Target: US Intelligence Watches Germany Closely (<http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html>), August 12, 2013.
87. "Snowden Interview: NSA and the Germans 'In Bed Together'" (<http://www.spiegel.de/international/world/edward-snowden-accuses-germany-of-aiding-nsa-in-spying-efforts-a-909847.html>). Spiegel International. July 7, 2013.
88. Campbell, Duncan. "Paper 1: Echelon and its role in COMINT" (<http://www.heise.de/tp/artikel/7/7747/1.html>). *heise online*. Retrieved March 11, 2015.
89. "NSA's global interception network" (<http://electrospace.blogspot.com/2013/12/nsas-global-interception-network.html>). *electrospace.net*. July 17, 2014. Retrieved March 11, 2015.
90. "NSA Satellite Communications SIGINT Station in Thailand Found" (<http://www.matthewaid.com/post/56608069320/nsa-satellite-communications-sigint-station-in>). *matthewaid.com*. July 27, 2013. Retrieved March 11, 2015.
91. "Thai map" (<https://www.google.com/maps/@16.4755559,102.8442837,171m/data=!3m1!1e3?hl=en>). *Google Maps*. Retrieved March 11, 2015.
92. Sabar, Ariel (July 20, 2013). "Congress curbs NSA's power to contract with suppliers" ([http://articles.baltimoresun.com/2003-07-20/news/0307200276\\_1\\_nsa-eavesdropping-agency](http://articles.baltimoresun.com/2003-07-20/news/0307200276_1_nsa-eavesdropping-agency)). *Baltimore Sun*. Tribune Company. Retrieved June 17, 2013.
93. Author redacted (circa 1983, partially declassified April 21, 2021). "The NSA Comes Out of the Closet: The Debate over Public Cryptography in the Inman Era (U)" (<https://cryptome.org/2021/04/Joseph-Meyer-IEEE-1977.pdf>) (PDF). *Cryptologic Quarterly*. U.S. National Security Agency. "Public cryptography issues were overwhelming Inman and the NSA. (p.12)" Check date values in: |date= (help)

94. Weeks, Bryan; et al. "Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms" (<https://web.archive.org/web/20111024234406/http://csrc.nist.gov/archive/aes/round2/NSA-AESfinalreport.pdf>) (PDF). National Institute of Standards and Technology. Archived from the original (<http://csrc.nist.gov/archive/aes/round2/NSA-AESfinalreport.pdf>) (PDF) on 2011-10-24. Retrieved June 29, 2013.
95. "the NIST standards that define Suite B..." in "Suite B Cryptography / Cryptographic Interoperability" ([https://web.archive.org/web/20160101091229/https://www.nsa.gov/ia/programs/suiteb\\_cryptography/](https://web.archive.org/web/20160101091229/https://www.nsa.gov/ia/programs/suiteb_cryptography/)). National Security Agency. Archived from the original ([https://www.nsa.gov/ia/programs/suiteb\\_cryptography/](https://www.nsa.gov/ia/programs/suiteb_cryptography/)) on 2016-01-01. Retrieved June 29, 2013.
96. Committee on C4ISR for Future Naval Strike Groups, National Research Council (2006). *C4ISR for Future Naval Strike Groups* (<https://books.google.com/books?id=NByKhCK3edkC&pg=PA167>). National Academies Press. p. 167. ISBN 978-0-309-09600-3.
97. "Adkins Family asked for a pic of the KL-7. Here you go!..." in "NSA – National Cryptologic Museum" (<https://www.facebook.com/NationalCryptologicMuseum>). Facebook. March 20, 2013. Retrieved June 30, 2013.
98. "Cryptographic Damage Assessment: DOCID: 3997687" ([https://web.archive.org/web/20130918031554/http://www.nsa.gov/public\\_info/\\_files/uss\\_pueblo/Section\\_V\\_Cryptographic\\_Damage\\_Assessment.pdf](https://web.archive.org/web/20130918031554/http://www.nsa.gov/public_info/_files/uss_pueblo/Section_V_Cryptographic_Damage_Assessment.pdf)) (PDF). National Security Agency. 1968. Archived from the original ([https://www.nsa.gov/public\\_info/\\_files/uss\\_pueblo/Section\\_V\\_Cryptographic\\_Damage\\_Assessment.pdf](https://www.nsa.gov/public_info/_files/uss_pueblo/Section_V_Cryptographic_Damage_Assessment.pdf)) (PDF) on September 18, 2013. Retrieved June 30, 2013.
99. "Cryptologic Excellence: Yesterday, Today and Tomorrow" ([https://web.archive.org/web/20130918014341/http://www.nsa.gov/about/\\_files/cryptologic\\_heritage/publications/misc/50th\\_anniversary.pdf](https://web.archive.org/web/20130918014341/http://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/50th_anniversary.pdf)) (PDF). National Security Agency. 2002. p. 17. Archived from the original ([https://www.nsa.gov/about/\\_files/cryptologic\\_heritage/publications/misc/50th\\_anniversary.pdf](https://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/50th_anniversary.pdf)) (PDF) on 2013-09-18. Retrieved June 30, 2013.
00. Hickey, Kathleen (January 6, 2010). "NSA certifies Sectera Viper phone for classified communications" (<http://gcn.com/articles/2010/01/06/nsa-certifies-viper-for-classified-communications.aspx>). GCN. 1105 Media. Retrieved June 30, 2013.
01. "JITC Networks, Transmissions, and Integration Division Electronic Key Management System (EKMS)" (<https://web.archive.org/web/20130515225818/http://jitc.fhu.disa.mil/ekms/>). U.S. Department of Defense: Defense Information Systems Agency: Joint Interoperability Certifier. February 1991. Archived from the original (<http://jitc.fhu.disa.mil/ekms/>) on May 15, 2013. Retrieved June 30, 2013.
02. "6.2.6 What is Fortezza?" (<https://web.archive.org/web/20120715221703/http://www.rsa.com/rsalabs/node.asp?id=2320>). RSA Laboratories, EMC Corporation. Archived from the original (<http://www.rsa.com/rsalabs/node.asp?id=2320>) on July 15, 2012. Retrieved June 30, 2013.
03. "AN/ARC-231 Airborne Communication System" (<http://www.raytheon.com/capabilities/products/arc231/>). Raytheon. Retrieved June 30, 2013.
04. "NSA approves TACLANE-Router" ([http://www.upi.com/Business\\_News/Security-Industry/2007/10/24/NSA-approves-TACLANE-Router/UPI-47061193262728/](http://www.upi.com/Business_News/Security-Industry/2007/10/24/NSA-approves-TACLANE-Router/UPI-47061193262728/)). United Press International. October 24, 2007. Retrieved June 30, 2013.
05. Draft NIST SP 800-131, June 2010.
06. Lorenzo, Joseph (September 24, 2013). "What the heck is going on with NIST's cryptographic standard, SHA-3? | Center for Democracy & Technology" (<https://www.cdt.org/blogs/joseph-lorenzo-hall/2409-nist-sha-3>). Cdt.org. Retrieved October 9, 2013.
07. "Twitter / marshray: Believe it or not, NIST is" (<https://twitter.com/marshray/status/380800393367674880>). Twitter.com. Retrieved October 9, 2013.
08. "kelsey-invited-ches-0820.pdf – Google Drive" (<https://docs.google.com/file/d/0BzRYQSHuUMYOQXdHWkRiZXIURVE/>). Retrieved October 9, 2013.
09. Baker, Stewart A. "Don't Worry Be Happy" ([https://www.wired.com/wired/archive/2.06/nsa.clipper\\_pr.html](https://www.wired.com/wired/archive/2.06/nsa.clipper_pr.html)). *Wired*. 2 (6). Retrieved June 28, 2013.

10. "Key Escrow, Key Recovery, Trusted Third Parties & Govt. Access to Keys" ([https://web.archive.org/web/20120429112956/http://w2.eff.org/Privacy/Key\\_escrow/](https://web.archive.org/web/20120429112956/http://w2.eff.org/Privacy/Key_escrow/)). Electronic Frontier Foundation. Archived from the original ([https://w2.eff.org/Privacy/Key\\_escrow/](https://w2.eff.org/Privacy/Key_escrow/)) on April 29, 2012. Retrieved June 28, 2013.
11. Schneier, Bruce (July 15, 1998). "Declassifying Skipjack" (<http://www.schneier.com/crypto-gram-9807.html#skip>). Crypto-Gram (schneier.com). Retrieved June 28, 2013.
12. "SKIPJACK and KEA Algorithm Specifications" (<https://web.archive.org/web/20111021070535/http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf>) (PDF). National Institute of Standards and Technology. May 29, 1998. Archived from the original (<http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf>) (PDF) on 2011-10-21. Retrieved June 28, 2013.
13. Schneier, Bruce (November 15, 2007). "Did NSA Put a Secret Backdoor in New Encryption Standard?" ([https://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters\\_1115](https://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115)). *Wired News*. Archived ([https://web.archive.org/web/20121024090318/http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters\\_1115](https://web.archive.org/web/20121024090318/http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115)) from the original on October 24, 2012. Retrieved July 4, 2008.
14. Matthew Green (September 18, 2013). "A Few Thoughts on Cryptographic Engineering: The Many Flaws of Dual\_EC\_DRBG" (<http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html>). Blog.cryptographyengineering.com. Retrieved October 9, 2013.
15. "Dual\_Ec\_Drbg backdoor: a proof of concept at Aris' Blog – Computers, ssh and rock'n roll" (<http://blog.0xbadc0de.be/archives/155>). *0xbadc0de.be*.
16. "itlbul2013 09 Supplemental" (<https://web.archive.org/web/20131008170739/http://www.propublica.org/documents/item/785571-itlbul2013-09-supplemental#document/p2>). ProPublica. Archived from the original (<https://www.propublica.org/documents/item/785571-itlbul2013-09-supplemental#document/p2>) on October 8, 2013. Retrieved October 9, 2013.
17. Matthew Green (September 20, 2013). "A Few Thoughts on Cryptographic Engineering: RSA warns developers not to use RSA products" (<http://blog.cryptographyengineering.com/2013/09/rsa-warns-developers-against-its-own.html>). Blog.cryptographyengineering.com. Retrieved October 9, 2013.
18. NSA Denies It Will Spy on Utilities (<https://www.wired.com/threatlevel/2010/07/nsa-perfect-citizen-denial/>), Threat Level, Wired.com
19. Mick, Jason (July 8, 2010). "DailyTech – NSA's "Perfect Citizen" Program: Big Brother or Cybersecurity Savior?" (<https://web.archive.org/web/20100711071346/http://www.dailytech.com/NSAs+Perfect+Citizen+Program++Big+Brother+or+Cybersecurity+Savior/article18969.htm>). *DailyTech*. Archived from the original (<http://www.dailytech.com/NSAs+Perfect+Citizen+Program++Big+Brother+or+Cybersecurity+Savior/article18969.htm>) on July 11, 2010. Retrieved July 8, 2010.
20. Whitney, Lance (July 8, 2010). "Report: NSA initiating program to detect cyberattacks" ([http://news.cnet.com/8301-1009\\_3-20009952-83.html](http://news.cnet.com/8301-1009_3-20009952-83.html)). *CNET.com*. Retrieved July 8, 2010.
21. Gorman, Siobhan (July 7, 2010). "U.S. Program to Detect Cyber Attacks on Infrastructure" ([http://www.wsj.com/articles/SB10001424052748704545004575352983850463108?mod=WSJ\\_hpp\\_MIDDLETopStories](http://www.wsj.com/articles/SB10001424052748704545004575352983850463108?mod=WSJ_hpp_MIDDLETopStories)). *The Wall Street Journal*. Retrieved July 7, 2010.
22. Robyn Winder & Charlie Speight (April 19, 2013). "Untangling the Web: A Guide to Internet Research" ([https://web.archive.org/web/20130509043240/http://www.nsa.gov/public\\_info/files/Untangling\\_the\\_Web.pdf](https://web.archive.org/web/20130509043240/http://www.nsa.gov/public_info/files/Untangling_the_Web.pdf)) (PDF). *National Security Agency Public Information*. Archived from the original ([https://www.nsa.gov/public\\_info/files/Untangling\\_the\\_Web.pdf](https://www.nsa.gov/public_info/files/Untangling_the_Web.pdf)) (PDF) on May 9, 2013. Retrieved May 9, 2013.
23. Zetter, Kim (May 9, 2013). "Use These Secret NSA Google Search Tips to Become Your Own Spy Agency" (<https://www.wired.com/threatlevel/2013/05/nsa-manual-on-hacking-internet/>). *Wired Magazine*.
24. Schneier, Bruce (1996). *Applied Cryptography, Second Edition*. John Wiley & Sons. pp. 609–610. ISBN 978-0-471-11709-4.

25. "United States Patent 6,947,978 – Method for geolocating logical network addresses" (<http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=%2Fnetacgi%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN%2F6947978>). United States Patent and Trademark Office. September 20, 2005. Retrieved July 4, 2008.
26. James Risen and Eric Lichtblau (June 10, 2013). "How the U.S. Uses Technology to Mine More Data More Quickly" (<https://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agency-cys-wider-reach.html?pagewanted=all>). *The New York Times*. Retrieved June 13, 2013.
27. "Frequently Asked Questions About NSA: 9. Can you explain the NSA and CSS seals?" ([http://www.nsa.gov/about/faqs/about\\_nsa.shtml#about9](http://www.nsa.gov/about/faqs/about_nsa.shtml#about9)). National Security Agency. Retrieved July 18, 2013.
28. "History of The Insignia" ([https://www.nsa.gov/about/cryptologic\\_heritage/center\\_crypt\\_history/insignia/index.shtml](https://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/insignia/index.shtml)). National Security Agency. Retrieved July 18, 2013.
29. "The National Security Agency Insignia" (<https://web.archive.org/web/20080413063307/http://www.nsa.gov/history/histo00018.cfm>). National Security Agency via Internet Archive. Archived from the original (<https://www.nsa.gov/history/histo00018.cfm>) on April 13, 2008. Retrieved July 18, 2013.
30. "A Dangerous Business: The U.S. Navy and National Reconnaissance During the Cold War" ([https://web.archive.org/web/20130918005012/http://www.nsa.gov/about\\_files/cryptologic\\_heritage/publications/coldwar/dangerous\\_business.pdf](https://web.archive.org/web/20130918005012/http://www.nsa.gov/about_files/cryptologic_heritage/publications/coldwar/dangerous_business.pdf)) (PDF). National Security Agency. Archived from the original ([https://www.nsa.gov/about\\_files/cryptologic\\_heritage/publications/coldwar/dangerous\\_business.pdf](https://www.nsa.gov/about_files/cryptologic_heritage/publications/coldwar/dangerous_business.pdf)) (PDF) on 2013-09-18. Retrieved June 13, 2013.
31. "National Cryptologic Memorial (List of Names) – NSA/CSS" ([https://www.nsa.gov/about/cryptologic\\_heritage/memorial\\_wall/memorial\\_wall\\_list.shtml](https://www.nsa.gov/about/cryptologic_heritage/memorial_wall/memorial_wall_list.shtml)). NSA.gov. Retrieved June 13, 2013.
32. Echelon and the Legal Restraints on Signals Intelligence: A Need For Reevaluation (<http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1113&context=dlj>) by Lawrence D. Sloan on April 30, 2001
33. Liu, Edward C. et. al. (May 21, 2015) Overview of Constitutional Challenges to NSA Collection Activities (<https://fas.org/sgp/crs/intel/R43459.pdf>). Washington, DC: Congressional Research Service.
34. "Obama's changes to NSA data collection published on February 5, 2015, by Christina Murray quoting David E. Sanger of *The New York Times*" (<https://www.nytimes.com/2015/02/03/world/president-tweaks-the-rules-on-data-collection.html>).
35. Savage, Charlie (2019-03-04). "Disputed N.S.A. Phone Program Is Shut Down, Aide Says" (<https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html>). *The New York Times*. ISSN 0362-4331 (<https://www.worldcat.org/issn/0362-4331>). Retrieved 2019-03-06.
36. James Risen & Eric Lichtblau (December 16, 2005), Bush Lets U.S. Spy on Callers Without Courts (<https://www.nytimes.com/2005/12/16/politics/16program.html>), *The New York Times*
37. "Gwu.edu" (<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index2.html>). Gwu.edu. Retrieved October 9, 2013.
38. "6th Circuit Court of Appeals Decision" (<https://web.archive.org/web/20130117053024/http://fl1.findlaw.com/news.findlaw.com/nytimes/docs/nsa/aclunsa70607opn.pdf>) (PDF). Archived from the original (<http://fl1.findlaw.com/news.findlaw.com/nytimes/docs/nsa/aclunsa70607opn.pdf>) (PDF) on January 17, 2013. Retrieved October 9, 2013.
39. Mike Rosen-Molina (May 19, 2007). "Ex-Guantanamo lawyers sue for recordings of client meetings" (<https://web.archive.org/web/20080502051556/http://jurist.law.pitt.edu/paperchase/2007/05/ex-guantanamo-lawyers-sue-for.php>). The Jurist. Archived from the original (<http://jurist.law.pitt.edu/paperchase/2007/05/ex-guantanamo-lawyers-sue-for.php>) on May 2, 2008. Retrieved May 22, 2007.
40. "CCR v. Bush" (<http://ccrjustice.org/ourcases/current-cases/ccr-v.-bush>). Center for Constitutional Rights. Retrieved June 15, 2009.

41. KJ Mullins (September 20, 2008). "Jewel Vs. NSA Aims To Stop Illegal Surveillance" (<http://www.digitaljournal.com/article/260075>). *Digital Journal*. Retrieved December 30, 2011.
42. *Jewel v. NSA* (complaint) (<https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf>). September 18, 2008. Electronic Frontier Foundation. Retrieved December 30, 2011.
43. Kravets, David (July 15, 2009). "Obama Claims Immunity, As New Spy Case Takes Center Stage" (<https://www.wired.com/threatlevel/2009/07/jewel/>). *Wired*. Retrieved December 30, 2011.
44. Van Loo, Rory (2019-10-01). "The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance" ([https://scholarship.law.bu.edu/faculty\\_scholarship/678](https://scholarship.law.bu.edu/faculty_scholarship/678)). *Vanderbilt Law Review*. **72** (5): 1563.
45. "For Your Eyes Only?" (<https://www.pbs.org/shows/307/index.html>). *NOW*. February 16, 2007. on PBS
46. Gorman, Siobahn (March 10, 2008). "NSA's Domestic Spying Grows As Agency Sweeps Up Data" ([https://web.archive.org/web/20090124141023/http://online.wsj.com/public/article\\_print/SB120511973377523845.html](https://web.archive.org/web/20090124141023/http://online.wsj.com/public/article_print/SB120511973377523845.html)). The Wall Street Journal Online. Archived from the original (<http://www.wsj.com/articles/SB120511973377523845>) on January 24, 2009. Retrieved March 14, 2014.
47. Liberty and Security in a Changing World ([https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12\\_rg\\_final\\_report.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf)) Archived ([https://web.archive.org/web/20170124173532/https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12\\_rg\\_final\\_report.pdf](https://web.archive.org/web/20170124173532/https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf)) 2017-01-24 at the Wayback Machine – Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 12, 2013, 308 pages
48. Mark Hosenball; Will Dunham (April 11, 2014). "White House, spy agencies deny NSA exploited 'Heartbleed' bug" (<https://web.archive.org/web/20140415175914/http://www.reuters.com/article/2014/04/11/us-cybersecurity-internet-bug-nsa-idUSBREA3A1XD20140411>). *Reuters*. Archived from the original (<https://www.reuters.com/article/2014/04/11/us-cybersecurity-internet-bug-nsa-idUSBREA3A1XD20140411>) on April 15, 2014. Retrieved April 16, 2014.
49. John Shiffman and Kristina Cooke (August 5, 2013) *Exclusive: U.S. directs agents to cover up program used to investigate Americans* (<https://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>) Archived (<https://web.archive.org/web/20130814032628/http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>) 2013-08-14 at the Wayback Machine. *Reuters*. Retrieved August 12, 2013.
50. John Shiffman and David Ingram (August 7, 2013) *Exclusive: IRS manual detailed DEA's use of hidden intel evidence* (<http://uk.reuters.com/article/2013/08/07/uk-dea-irs-idUKBRE9761B620130807>). *Reuters*. Retrieved August 12, 2013.
51. Lichtblau, Eric & Risen, James (April 15, 2009). "N.S.A.'s Intercepts Exceed Limits Set by Congress" (<https://www.nytimes.com/2009/04/16/us/16nsa.html>). *The New York Times*. Retrieved April 15, 2009.
52. Ackerman, Spencer (April 16, 2009). "NSA Revelations Spark Push to Restore FISA" (<https://web.archive.org/web/20090418170843/http://washingtonindependent.com/39153/nsa-revelations-spark-movement-to-restore-fisa>). *The Washington Independent*. Center for Independent Media. Archived from the original (<http://washingtonindependent.com/39153/nsa-revelations-spark-movement-to-restore-fisa>) on April 18, 2009. Retrieved April 19, 2009.
53. "Statistics on whether the NSA's Secret Data Collection is Acceptable" (<http://www.statista.com/statistics/260140/opinion-of-americans-on-whether-the-nsas-secret-data-collection-is-acceptable/>). Statista. Retrieved July 19, 2013.
54. "59% Oppose Government's Secret Collecting of Phone Records" ([http://www.rasmussenreport.com/public\\_content/politics/general\\_politics/june\\_2013/59\\_oppose\\_government\\_s\\_secret\\_collecting\\_of\\_phone\\_records](http://www.rasmussenreport.com/public_content/politics/general_politics/june_2013/59_oppose_government_s_secret_collecting_of_phone_records)). Rasmussen Reports. June 9, 2013. Retrieved July 19, 2013.

55. Newport, Frank (June 12, 2013). "Americans Disapprove of Government Surveillance Programs" (<http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx>). Gallup. Retrieved July 19, 2013.
56. "Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic" (<http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/>). Pew Research Center. June 10, 2013. Retrieved July 19, 2013.
57. Glenn Greenwald (June 6, 2013). "Revealed: NSA collecting phone records of millions of Americans daily" (<https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>). *The Guardian*. London. Retrieved June 6, 2013.
58. Charlie Savage, Edward Wyatt (2013-06-05). "U.S. Is Secretly Collecting Records of Verizon Calls" (<https://www.nytimes.com/2013/06/06/us/us-secretly-collecting-logs-of-business-calls.html>). *The New York Times*.
59. Savage, Charlie (August 8, 2013). "N.S.A. Said to Search Content of Messages to and From U.S." (<https://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html>). *The New York Times*. Retrieved August 13, 2013.
60. Nakashima, Ellen. "NSA phone record collection does little to prevent terrorist attacks, group says" ([https://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2\\_story.html/](https://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html/)), *The Washington Post*, January 12, 2014
61. Nakashima, Ellen. / "NSA chief defends collecting Americans' data" ([https://www.washingtonpost.com/world/national-security/nsa-chief-defends-collecting-americans-data/2013/09/25/5db2583c-25f1-11e3-b75d-5b7f66349852\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-chief-defends-collecting-americans-data/2013/09/25/5db2583c-25f1-11e3-b75d-5b7f66349852_story.html)), *The Washington Post*, September 25, 2013
62. Read "Engaging Privacy and Information Technology in a Digital Age" at NAP.edu (<https://www.nap.edu/read/11896/chapter/11>).
63. Federal judge rules NSA program is likely unconstitutional (<https://apps.washingtonpost.com/page/world/federal-judge-rules-nsa-program-is-likely-unconstitutional/668/>), *The Washington Post*, December 16, 2013
64. New Rules for the National Security Agency ([https://www.washingtonpost.com/opinions/the-nsa-went-too-far/2015/05/10/02635924-f5aa-11e4-b2f3-af5479e6bbdd\\_story.html](https://www.washingtonpost.com/opinions/the-nsa-went-too-far/2015/05/10/02635924-f5aa-11e4-b2f3-af5479e6bbdd_story.html)) by the Editorial Board on May 10, 2015
65. Charlie Savage, Jonathan Weisman (2015-05-07). "N.S.A. Collection of Bulk Call Data is Ruled Illegal" (<https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html>). *The New York Times*.
66. "Rand Paul vs. Washington DC on the USA Freedom Act" (<https://web.archive.org/web/20150602001207/http://hotair.com/standing-athwarth-history-yelling-stop/2015/05/31/rand-paul-vs-washington-dc-on-the-usa-freedom-act/>). *HotAir*. Archived from the original (<http://hotair.com/standing-athwarth-history-yelling-stop/2015/05/31/rand-paul-vs-washington-dc-on-the-usa-freedom-act/>) on 2015-06-02. Retrieved 2015-06-02.
67. Top Level Telecommunications, Slides about NSA's Upstream collection (<http://electrospace.blogspot.com/2014/01/slides-about-nsas-upstream-collection.html>), January 17, 2014
68. NSA paying U.S. companies for access to communications networks ([https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html)) by Craig Timberg and Barton Gellman on August 29, 2013
69. NSA PRISM Controversy: Apple, Facebook, Google, more deny knowledge (<http://www.digitalspy.com/tech/news/a487943/nsa-prism-controversy-apple-facebook-google-more-deny-knowledge.html#~pbKCS2AUgt8krC>) by Digital Spy on June 6, 2013
70. Microsoft, Facebook, Google and Yahoo release US surveillance requests (<https://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests>) by Spencer Ackerman and Dominic Rushe on February 3, 2014

71. *Memorandum of the United States in Response to the Court's Order Dated January 28, 2009* ([http://www.dni.gov/files/documents/section/pub\\_Feb%2012%202009%20Memorandum%20of%20US.pdf](http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf)) (PDF). Washington DC: Foreign Intelligence Surveillance Court Washington DC. January 28, 2009. p. 11.
72. Greenberg, Andy. "NSA Secretly Admitted Illegally Tracking Thousands Of 'Alert List' Phone Numbers For Years" (<https://www.forbes.com/sites/andygreenberg/2013/09/10/nsa-secretly-admitted-illegally-tracking-thousands-of-alert-list-phone-numbers-for-years/>). *Forbes*. Retrieved February 25, 2014.
73. Brandon, Russel. "NSA illegally searched 15,000 suspects' phone records, according to declassified report" (<https://www.theverge.com/2013/9/10/4716642/nsa-illegally-searched-15000-suspects-phone-records-according-to>). *The Verge*. Retrieved February 25, 2014.
74. Timm, Trevor. "Government Releases NSA Surveillance Docs and Previously Secret FISA Court Opinions in Response to EFF Lawsuit" (<https://www.eff.org/deeplinks/2013/09/government-releases-nsa-surveillance-docs-and-previously-secret-fisa-court>). Electronic Frontier Foundation. Retrieved February 25, 2014.
75. Barton Gellman and Ashton Solanti, December 5, 2013, "NSA tracking cellphone locations worldwide, Snowden documents show" ([https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac\\_story.html?hpid=z1](https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html?hpid=z1)), *The Washington Post*. Retrieved December 7, 2013.
76. Greenwald, Glenn; MacAskill, Ewen (June 6, 2013). "NSA Prism program taps in to user data of Apple, Google and others" (<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>). *The Guardian*. Retrieved June 15, 2013.
77. Gellman and Soltani, October 15, 2013 "NSA collects millions of e-mail address books globally" ([https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html)), *The Washington Post*. Retrieved October 16, 2013.
78. Perlroth, Larson and Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web" (<https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>), *The New York Times* September 5, 2013. Retrieved September 23, 2013.
79. Arthur, Charles "Academics criticise NSA and GCHQ for weakening online encryption" (<https://www.theguardian.com/technology/2013/sep/16/nsa-gchq-undermine-internet-security>), *The Guardian* September 16, 2013. Retrieved September 23, 2013.
80. "Senators: Limit NSA snooping into US phone records" (<http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records>). Associated Press. Retrieved October 15, 2013. ""Is it the goal of the NSA to collect the phone records of all Americans?" Udall asked at Thursday's hearing. "Yes, I believe it is in the nation's best interest to put all the phone records into a lockbox that we could search when the nation needs to do it. Yes," Alexander replied."
81. Glenn Greenwald (June 6, 2013). "NSA collecting phone records of millions of Verizon customers daily" (<https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>). *The Guardian*. Retrieved September 16, 2013.
82. Court Reveals 'Secret Interpretation' Of The Patriot Act, Allowing NSA To Collect All Phone Call Data (<https://www.techdirt.com/articles/20130917/13395324556/court-reveals-secret-interpretation-patriot-act-allowing-nsa-to-collect-all-phone-call-data.shtml>), September 17, 2013. Retrieved September 19, 2013.
83. "Exclusive: U.S. directs agents to cover up program used to investigate Americans" (<https://web.archive.org/web/20130814032628/http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>). *Reuters*. August 5, 2013. Archived from the original (<https://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>) on August 14, 2013. Retrieved August 14, 2013.

84. Glenn Greenwald, Ryan Gallagher & Ryan Grim, November 26, 2013, "[Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'](http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html)" ([http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims\\_n\\_4346128.html](http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html)), *Huffington Post*. Retrieved November 28, 2013.
85. "Vast majority of NSA spy targets are mistakenly monitored" (<https://web.archive.org/web/20140714180053/http://www.philadelphianews.net/index.php/sid/223558101/scat/c08dd24cec417021/ht/Vast-majority-of-NSA-spy-targets-are-mistakenly-monitored>). Philadelphia News.Net. Archived from the original (<http://www.philadelphianews.net/index.php/sid/223558101/scat/c08dd24cec417021/ht/Vast-majority-of-NSA-spy-targets-are-mistakenly-monitored>) on 2014-07-14. Retrieved July 7, 2014.
86. Greenwald, Glen, "Members of Congress denied access to basic information about NSA (<http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access>)", *The Guardian*, August 4, 2013. Retrieved September 23, 2013.
87. Loennig, C., "Court: Ability to police U.S. spying program limited ([https://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125\\_story.html](https://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html))", *The Washington Post*, August 16, 2013. Retrieved September 23, 2013.
88. Gellman, B. NSA broke privacy rules thousands of times per year, audit finds ([https://articles.washingtonpost.com/2013-08-15/world/41431831\\_1\\_washington-post-national-security-agency-documents](https://articles.washingtonpost.com/2013-08-15/world/41431831_1_washington-post-national-security-agency-documents)) Archived ([https://web.archive.org/web/20131218210342/http://articles.washingtonpost.com/2013-08-15/world/41431831\\_1\\_washington-post-national-security-agency-documents](https://web.archive.org/web/20131218210342/http://articles.washingtonpost.com/2013-08-15/world/41431831_1_washington-post-national-security-agency-documents)) 2013-12-18 at the *Wayback Machine*, *The Washington Post*, August 15, 2013. Retrieved September 23, 2013.
89. Gorman, S. NSA Officers Spy on Love Interests (<https://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/>), Wall St Journal, August 23, 2013. Retrieved September 23, 2013.
90. Andrea Peterson, LOVEINT: When NSA officers use their spying power on love interests (<http://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/>), *The Washington Post* (August 24, 2013).
91. Spencer Ackerman, November 19, 2013, "Fisa court documents reveal extent of NSA disregard for privacy restrictions (<https://www.theguardian.com/world/2013/nov/19/fisa-court-documents-nsa-violations-privacy>)", *The Guardian*. Retrieved November 21, 2013.
92. John D Bates (October 3, 2011). "[redacted]" ([https://www.eff.org/sites/default/files/filenode/fisc\\_opinion\\_-\\_unconstitutional\\_surveillance\\_0.pdf](https://www.eff.org/sites/default/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf)). p. 16.
93. Ellen Nakashima, Julie Tate and Carol Leonnig (September 10, 2013). "Declassified court documents highlight NSA violations in data collection for surveillance ([https://www.washingtonpost.com/world/national-security/declassified-court-documents-highlight-nsa-violations/2013/09/10/60b5822c-1a4b-11e3-a628-7e6dde8f889d\\_story.html](https://www.washingtonpost.com/world/national-security/declassified-court-documents-highlight-nsa-violations/2013/09/10/60b5822c-1a4b-11e3-a628-7e6dde8f889d_story.html))". *The Washington Post*. Retrieved September 14, 2013.
94. Richard Leon, December 16, 2013, *Memorandum Opinion, Klayman vs. Obama* (<https://www.theguardian.com/world/interactive/2013/dec/16/nsa-collection-phone-metadata-district-court-ruling>). U.S. District Court for the District of Columbia. Reproduced on The Guardian website. Retrieved February 3, 2013.
95. Bazzle, Steph (December 27, 2013). "Judge Says NSA's Data Collection Is Legal" (<https://web.archive.org/web/20131228162843/http://www.indyposted.com/227717/judge-says-nsas-data-collection-legal/>). Indyposted. Archived from the original (<http://www.indyposted.com/227717/judge-says-nsas-data-collection-legal/>) on December 28, 2013. Retrieved December 28, 2013.
96. Kessler, Glenn, James Clapper's 'least untruthful' statement to the Senate ([https://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459\\_blog.html](https://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html)), June 12, 2013. Retrieved September 23, 2013.

97. Glenn Greenwald, XKeyscore: NSA tool collects 'nearly everything a user does on the internet' (<https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>), *The Guardian* (July 31, 2013).
98. Kube, C., June 27, 2013, "NSA chief says surveillance programs helped foil 54 plots" ([http://usnews.nbcnews.com/\\_news/2013/06/27/19175466-nsa-chief-says-surveillance-programs-helped-foil-54-plots?lite](http://usnews.nbcnews.com/_news/2013/06/27/19175466-nsa-chief-says-surveillance-programs-helped-foil-54-plots?lite)), *US News on nbcnews.com*. Retrieved September 27, 2013.
99. "NSA Confirms Dragnet Phone Records Collection, But Admits It Was Key in Stopping Just 1 Terror Plot" ([http://www.democracynow.org/2013/8/1/nsa\\_confirms\\_dragnet\\_phone\\_records\\_collection](http://www.democracynow.org/2013/8/1/nsa_confirms_dragnet_phone_records_collection)), *Democracy Now* August 1, 2013. Retrieved September 27, 2013.
00. "Indictment: USA vs Basaaly Saeed Moalin, Mohamed Mohamed Mohamud and Issa Doreh" (<http://jnslp.files.wordpress.com/2010/11/moalin.pdf>). Southern District of California July 2010 Grand Jury. Retrieved September 30, 2013.
01. "54 Attacks in 20 Countries Thwarted By NSA Collection" (<https://web.archive.org/web/20131023153822/http://democrats.intelligence.house.gov/press-release/54-attacks-20-countries-thwarted-nsa-collection>) (Press release). The Permanent Select Committee on Intelligence. July 23, 2013. Archived from the original (<http://democrats.intelligence.house.gov/press-release/54-attacks-20-countries-thwarted-nsa-collection>) on October 23, 2013. Retrieved March 14, 2014.
02. "Senate caves, votes to give telecoms retroactive immunity" (<https://arstechnica.com/security/2008/02/democrats-fail-to-block-telecom-immunity-provision/>). *Ars Technica*. February 13, 2008. Retrieved September 16, 2013.
03. "Forget Retroactive Immunity, FISA Bill is also about Prospective Immunity" (<https://web.archive.org/web/20130918200841/http://progressive.org/mag/wx071008.html>). The Progressive. July 10, 2008. Archived from the original (<http://progressive.org/mag/wx071008.html>) on September 18, 2013. Retrieved September 16, 2013.
04. "Restricted Web access to the Guardian is Armywide, say officials" ([http://www.montereyherald.com/local/ci\\_23554739/restricted-web-access-guardian-is-army-wide-officials](http://www.montereyherald.com/local/ci_23554739/restricted-web-access-guardian-is-army-wide-officials)) Archived ([https://web.archive.org/web/20141020150616/http://www.montereyherald.com/local/ci\\_23554739/restricted-web-access-guardian-is-army-wide-officials](https://web.archive.org/web/20141020150616/http://www.montereyherald.com/local/ci_23554739/restricted-web-access-guardian-is-army-wide-officials)) 2014-10-20 at the Wayback Machine, Philipp Molnar, *Monterey Herald*, June 27, 2013. Retrieved October 15, 2014.
05. Ackerman, Spencer; Roberts, Dan (June 28, 2013). "US Army Blocks Access to Guardian Website to Preserve 'Network Hygiene'—Military Admits to Filtering Reports and Content Relating to Government Surveillance Programs for Thousands of Personnel" (<https://www.theguardian.com/world/2013/jun/28/us-army-blocks-guardian-website-access>). *The Guardian*. Retrieved June 30, 2013.
06. Ackerman, Spencer (July 1, 2013). "US military blocks entire Guardian website for troops stationed abroad" (<https://www.theguardian.com/world/2013/jul/01/us-military-blocks-guardian-troops>). *The Guardian*.
07. Greenwald, Glenn (October 16, 2014). "UN Report Finds Mass Surveillance Violates International Treaties and Privacy Rights" (<https://firstlook.org/theintercept/2014/10/15/un-investigator-report-condemns-mass-surveillance/>). Retrieved October 23, 2014.
08. Wong, Julia Carrie; Solon, Olivia (12 May 2017). "Massive ransomware cyber-attack hits 74 countries around the world" (<https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs>). *The Guardian*. Retrieved 12 May 2017.
09. Kharpal, Arjun (19 May 2017). "Cyberattack that hit 200,000 users was 'huge screw-up' by government, Wikipedia's Jimmy Wales says" (<https://www.cnbc.com/2017/05/19/wannacry-cyberattack-nsa-wikipedia-jimmy-wales.html>). CNBC. Retrieved 2 June 2017.
10. "How the United States Lost to Hackers" (<https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html>). *The New York Times*. Retrieved 6 February 2021.

## References

---

- Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, Random House Digital, Inc., December 18, 2007. ISBN 0-307-42505-3. Previously published as: Doubleday, 2001, ISBN 0-385-49907-8.
- Bauer, Craig P. *Secret History: The Story of Cryptology (Volume 76 of Discrete Mathematics and Its Applications)*. CRC Press, 2013. ISBN 1-4665-6186-6.
- Weiland, Matt and Sean Wilsey. *State by State*. HarperCollins, October 19, 2010. ISBN 0-06-204357-9.

## Further reading


---

- Adams, Sam, *War of Numbers: An Intelligence Memoir* Steerforth; new edition (June 1, 1998).
- Aid, Matthew, *The Secret Sentry: The Untold History of the National Security Agency*, 432 pages, ISBN 978-1-59691-515-2, Bloomsbury Press (June 9, 2009).
  - Mandatory Declassification Review (<https://www.archives.gov/files/declassification/iscap/pdf/2013-114-doc1.pdf>) - Interagency Security Classification Appeals Panel
- Bamford, James, *The Puzzle Palace*, Penguin Books, ISBN 0-14-006748-5.
- Bamford, James, *The New York Times*, December 25, 2005; *The Agency That Could Be Big Brother* (<https://www.nytimes.com/2005/12/25/weekinreview/25bamford.html?pagewanted=all>).
- Bamford, James, *The Shadow Factory*, Anchor Books, 2009, ISBN 978-0-307-27939-2.
- Hanyok, Robert J. (2002). *Spartans in Darkness: American SIGINT and the Indochina War, 1945–1975* (<https://fas.org/irp/nsa/spartans/index.html>). National Security Agency. Retrieved November 16, 2008.
- Jackson, David (June 18, 2013). "Obama: NSA surveillance programs are 'transparent' " (<http://www.usatoday.com/story/theoval/2013/06/18/obama-charlie-rose-program-nsa-surveillance/2433549/>). *USA Today*. Retrieved June 18, 2013.
- Johnson, Thomas R. (2008). *American Cryptology during the Cold War* (<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/>). National Security Agency: Center for Cryptological History. Retrieved November 16, 2008.
- Radden Keefe, Patrick, *Chatter: Dispatches from the Secret World of Global Eavesdropping*, Random House, ISBN 1-4000-6034-6.
- Kent, Sherman, *Strategic Intelligence for American Public Policy*.
- Kahn, David, *The Codebreakers*, 1181 pp., ISBN 0-684-83130-9. Look for the 1967 rather than the 1996 edition.
- Laqueur, Walter, *A World of secrets*.
- Liston, Robert A., *The Pueblo Surrender: a Covert Action by the National Security Agency*, ISBN 0-87131-554-8.
- Levy, Steven, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*, Penguin Books, ISBN 0-14-024432-8.
- Prados, John, *The Soviet estimate: U.S. intelligence analysis & Russian military strength*, hardcover, 367 pages, ISBN 0-385-27211-1, Dial Press (1982).
- Perro, Ralph J. "Interviewing With An Intelligence Agency (or, A Funny Thing Happened On The Way To Fort Meade) (<https://www.fas.org/irp/eprint/nsa-interview.pdf>)." (Archive (<https://web.archive.org/web/20130202180139/http://www.fas.org/irp/eprint/nsa-interview.pdf>)) Federation of American Scientists. November 2003. Updated January 2004. – About the experience of a candidate of an NSA job in pre-employment screening. "Ralph J. Perro" is a pseudonym that is a reference to Ralph J. Canine (*perro* is Spanish for "dog", and a dog is a type of canine)
- Shaker, Richard J. "The Agency That Came in from the Cold (<https://www.ams.org/profession/employment-services/emp-shaker>)." (Archive (<https://web.archive.org/web/20140125104431/http://www.ams.org/profession/employment-services/emp-shaker>) *Notices. American Mathematical Society*. May/June 1992 pp. 408–411.

- Tully, Andrew, *The Super Spies: More Secret, More Powerful than the CIA*, 1969, LC 71080912.
- Church Committee, *Intelligence Activities and the Rights of Americans: 1976 US Senate Report on Illegal Wiretaps and Domestic Spying by the FBI, CIA and NSA*, Red and Black Publishers (May 1, 2008).
- "Just what is the NSA? (<http://www.cnn.com/video/data/2.0/video/us/2013/06/07/lawrence-nsa-no-such-agency.cnn.html>)" (video) *CNN*. June 7, 2013.
- "The NSA Files" (<https://www.theguardian.com/world/the-nsa-files>). *The Guardian*. London. June 8, 2013.
- "National Security Agency Releases History of Cold War Intelligence Activities (<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/>)." George Washington University. National Security Archive Electronic Briefing Book No. 260. Posted November 14, 2008.
- "The Snowden Archive" (<https://theintercept.com/snowden-sidtoday/?orderBy=publishedTime&orderDirection=desc#archive>). *The Intercept*. London. June 8, 2013.

## External links

---

- Official website (<https://www.nsa.gov/>) 
  - National Security Agency – 60 Years of Defending Our Nation ([https://web.archive.org/web/20180623141614/https://www.nsa.gov/about/cryptologic\\_heritage/60th/book/NSA\\_60th\\_Anniversary.pdf](https://web.archive.org/web/20180623141614/https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf))
  - Records of the National Security Agency/Central Security Service (<https://www.archives.gov/research/guide-fed-records/groups/457.html>)
  - The National Security Archive at George Washington University (<http://www.gwu.edu/~nsarchiv/>)
  - "United States Intelligence Community: Who We Are / NSA section" ([https://web.archive.org/web/20060925221125/http://www.intelligence.gov/1-members\\_nsa.shtml](https://web.archive.org/web/20060925221125/http://www.intelligence.gov/1-members_nsa.shtml)). Archived from the original ([http://www.intelligence.gov/1-members\\_nsa.shtml](http://www.intelligence.gov/1-members_nsa.shtml)) on September 25, 2006.
  - National Security Agency (NSA) Archive (<https://archive.org/details/nsa-archive>) on the Internet Archive
- 

Retrieved from "[https://en.wikipedia.org/w/index.php?title=National\\_Security\\_Agency&oldid=1024711063](https://en.wikipedia.org/w/index.php?title=National_Security_Agency&oldid=1024711063)"

---

This page was last edited on 23 May 2021, at 18:29 (UTC).

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