

SILICON VALLEY IS TOTALLY BASED AROUND SPYING ON THE PUBLIC

Every electronic device has a spy circuit in it. The practice of mass surveillance in the United States dates back to wartime monitoring and censorship of international communications from, to, or which passed through the United States. After the First and Second World Wars, mass surveillance continued throughout the Cold War period, via programs such as the Black Chamber and Project SHAMROCK. The formation and growth of federal law-enforcement and intelligence agencies such as the FBI, CIA, and NSA institutionalized surveillance used to also silence political dissent, as evidenced by COINTELPRO projects which targeted various organizations and individuals. During the Civil Rights Movement era, many individuals put under surveillance orders were first labelled as integrationists, then deemed subversive, and sometimes suspected to be supportive of the communist model of the United States' rival at the time, the Soviet Union. Other targeted individuals and groups included Native American activists, African American and Chicano liberation movement activists, and anti-war protesters.

The formation of the international UKUSA surveillance agreement of 1946 evolved into the ECHELON collaboration by 1955^[1] of five English-speaking nations, also known as the Five Eyes, and focused on interception of electronic communications, with substantial increases in domestic surveillance capabilities.^[2]

Following the September 11th attacks of 2001, domestic and international mass surveillance capabilities grew immensely. Contemporary mass surveillance relies upon annual presidential executive orders declaring a continued State of National Emergency, first signed by George W. Bush on September 14, 2001 and then continued on an annual basis during the presidencies of Barack Obama, Joe Biden, and the first presidency of Donald Trump, with it still being active as of November 2024.^{[3][4]} Mass surveillance is also based on several subsequent national security Acts including the USA PATRIOT Act and FISA Amendment Act's PRISM surveillance program. Critics and political dissenters currently describe the effects of these acts, orders, and resulting database network of fusion centers as forming a veritable American police state that simply institutionalized the illegal COINTELPRO tactics used to assassinate dissenters and leaders from the 1950s onwards.^{[5][6][7]}

Additional surveillance agencies, such as the DHS and the position of Director of National Intelligence, have greatly escalated mass surveillance since 2001. A series of media reports in 2013 revealed more recent programs and techniques employed by

the US intelligence community.^{[8][9]} Advances in computer and information technology allow the creation of huge national databases that facilitate mass surveillance in the United States^[8] by DHS managed fusion centers, the CIA's Terrorist Threat Integration Center (TTIC) program, and the FBI's Terrorist Screening Database (TSDB).

Mass surveillance databases are also cited as responsible for profiling Latino Americans and contributing to "self-deportation" techniques, or physical deportations by way of the DHS's ICEGang national database.^[10]

After World War I, the US Army and State Department established the Black Chamber, also known as the Cipher Bureau, which began operations in 1919.^[11] The Black Chamber was headed by Herbert O. Yardley, who had been a leader in the Army's Military Intelligence program. Regarded as a precursor to the National Security Agency, it conducted peacetime decryption of material including diplomatic communications until 1929.^{[12][13]}

In the advent of World War II, the Office of Censorship was established. The wartime agency monitored "communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country".^[14] This included the 350,000 overseas cables and telegrams and 25,000 international telephone calls made each week.^{[15]:144} "Every letter that crossed international or U.S. territorial borders from December 1941 to August 1945 was subject to being opened and scoured for details."^[14]

With the end of World War II, Project SHAMROCK was established in 1945. The organization was created to accumulate telegraphic data entering and exiting from the United States.^{[12][16]} Major communication companies such as Western Union, RCA Global and ITT World Communications actively aided the project, allowing American intelligence officials to gain access to international message traffic.^[17] Under the project, and many subsequent programs, no precedent had been established for judicial authorization, and no warrants were issued for surveillance activities. The project was terminated in 1975.^[12]

President Harry S. Truman established the National Security Agency (NSA) in 1952 for the purposes of collecting, processing, and monitoring intelligence data.^[18] The existence of NSA was not known to people as the memorandum by President Truman was classified.^[19]

When the Citizens' Commission to Investigate the FBI published stolen FBI documents revealing abuse of intelligence programs in 1971, Senator Frank Church began an investigation into the programs that become known as the Church Committee. The committee sought to investigate intelligence abuses throughout the 1970s. Following a report provided by the committee outlining egregious abuse, in 1976 Congress established the Senate Select Committee on Intelligence. It would later be joined by

the Foreign Intelligence Surveillance Court in 1978.[12] The institutions worked to limit the power of the agencies, ensuring that surveillance activities remained within the rule of law.[20]

Following the attacks of September 11, 2001, Congress passed the Patriot Act to strengthen security and intelligence efforts. The act granted the President broad powers on the war against terror, including the power to bypass the FISA Court for surveillance orders in cases of national security. Additionally, mass surveillance activities were conducted alongside various other surveillance programs under the head of President's Surveillance Program.[21] Under pressure from the public, the warrantless wiretapping program was allegedly ended in January 2007.[22]

Many details about the surveillance activities conducted in the United States were revealed in the disclosure by Edward Snowden in June 2013.[23][24] Regarded as one of the biggest media leaks in the United States, it presented extensive details about the surveillance programs of the NSA, that involved interception of Internet data and telephonic calls from over a billion users, across various countries.[25][24]

National Security Agency (NSA)

[\[edit\]](#)



U.S. Army, those who protested against the [Vietnam War](#) were put on the NSA's "watch list".[17]

1947: The National Security Act was signed by President Truman, establishing a National Security Council.[26][27]

1949: The Armed Forces Security Agency was established to coordinate signal operations between military branches.[28]

1952: The National Security Agency (NSA) was officially established by President Truman by way of a National Security Council Intelligence Directive 9, dated Oct. 24, while the NSA officially came into existence days later on Nov. 4.[12] According to *The New York Times*, the NSA was created in "absolute secrecy" by President Truman,[29] whose surveillance-minded administration ordered, only six weeks after President Truman took office, wiretaps on the telephones of Thomas Gardiner Corcoran, a close advisor of Franklin D. Roosevelt.[30] The recorded conversations are currently kept at the Harry S.

Truman Presidential Library and Museum, along with other documents considered sensitive (≈233,600 pages).

Federal Bureau of Investigation (FBI)

[\[edit\]](#)

Institutional domestic surveillance was founded in 1896 with the National Bureau of Criminal Identification, which evolved by 1908 into the Bureau of Investigation, operated under the authority of the Department of Justice. In 1935, the FBI had grown into an independent agency under the direction of J. Edgar Hoover whose staff, through the use of wire taps, cable taps, mail tampering, garbage filtering and infiltrators, prepared secret FBI Index Lists on more than 10 million people by 1939.^[31]

Purported to be chasing 'communists' and other alleged subversives, the FBI used public and private pressure to destroy the lives of those it targeted during McCarthyism, including those lives of the Hollywood 10 with the Hollywood blacklist. The FBI's surveillance and investigation roles expanded in the 1950s while using the collected information to facilitate political assassinations, including the murders of Fred Hampton and Mark Clark in 1969. FBI is also directly connected to the bombings, assassinations, and deaths of other people including Malcolm X in 1963, Viola Liuzzo in 1965, Dr. Martin Luther King Jr. in 1968, Anna Mae Pictou Aquash in 1976, and Judi Bari in 1990.^[32]

As the extent of the FBI's domestic surveillance continued to grow, many celebrities were also secretly investigated by the bureau, including:

●**First Lady Eleanor Roosevelt** – A vocal critic of Hoover who likened the FBI to an 'American Gestapo' for its Index lists.^[31] Roosevelt also spoke out against anti-Japanese prejudice during the second world war, and was later a delegate to the United Nations and instrumental in creating the Universal Declaration of Human Rights. The 3,000-page FBI dossier on Eleanor Roosevelt reveals Hoover's close monitoring of her activities and writings, and contains retaliatory charges against her for suspected Communist activities.^{[33][34]}

●**Frank Sinatra** – His 1,300 page FBI dossier, dating from 1943, contains allegations about Sinatra's possible ties to the American Communist Party. The FBI spent several decades tracking Sinatra and his associates.^{[35][36]}

●**Marilyn Monroe** – Her FBI dossier begins in 1955 and continues up until the months before her death. It focuses mostly on her travels and associations, searching for signs of leftist views and possible ties to communism.^[37] Her ex-husband, Arthur Miller, was also monitored.^[citation needed] Monroe's FBI dossier is "heavily censored", but a "reprocessed" version has been released by the FBI to the public.^[37]

●**John Lennon** – In 1971, shortly after Lennon arrived in the United States on a visa to meet up with anti-war activists, the FBI placed Lennon under surveillance, and the U.S. government tried to deport him from the country.[38] At that time, opposition to the Vietnam War had reached a peak and Lennon often showed up at political rallies to sing his anti-war anthem "*Give Peace a Chance*".[38] The U.S. government argued that Lennon's 300 page FBI dossier was particularly sensitive because its release may "lead to foreign diplomatic, economic and military retaliation against the United States",[39] and therefore only approved a "heavily censored" version.[40]

●**The Beatles**, of which John Lennon was a member, had a separate FBI dossier.



Some of the greatest historical figures of the 20th century, including several U.S. citizens, were placed under warrantless surveillance for the purpose of character assassination – a process that aims to destroy the credibility and reputation of a person, institution, or nation.

Left: Albert Einstein, who supported the anti-war movement and opposed nuclear proliferation, was a member of numerous civil rights groups including the National Association for the Advancement of Colored People (See Albert Einstein's political views). As a result of his political views, Einstein was subjected to telephone tapping, and his mail was searched by the U.S. Federal Bureau of Investigation (FBI) as part of a secret government campaign that aimed to link him with a Soviet espionage ring in order to first discredit him, and then deport him (unsuccessfully) from the United States.[41][42][43]

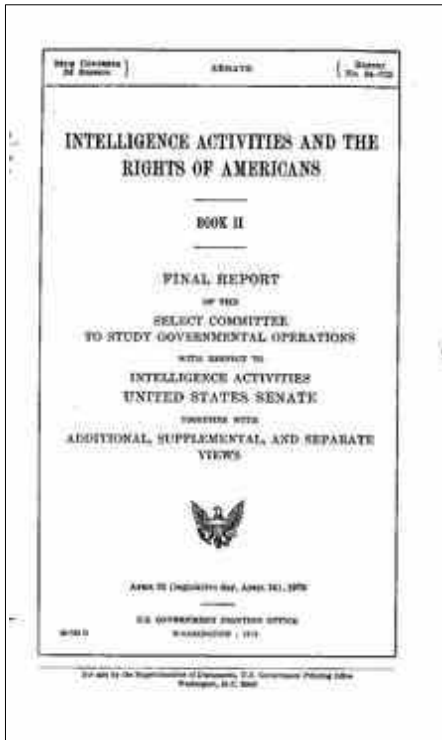
Center: Martin Luther King Jr., a leader of the Civil Rights Movement, was the target of an intensive campaign by the FBI to "neutralize" him as an effective civil rights activist.[44] An FBI memo recognized King to be the "most dangerous and effective Negro leader in the country.",[45] and the agency wanted to discredit him by collecting evidence to (unsuccessfully) prove that he had been influenced by communism.[45]

Right: Daniel Ellsberg, who leaked the Pentagon Papers to the media in 1971, experienced one of the most spectacular episodes of government surveillance and character assassination. The White House tried to steal his medical records and other possibly detrimental information by sending a special unit to break into the office of Ellsberg's psychiatrist.[46][47] These activities were later

uncovered during the course of investigation as the Watergate scandal slowly unfolded, which eventually led to the resignation of President Richard Nixon.[48]

See also: The FBI kept a dossier on Albert Einstein (≈1,500 pages) and Martin Luther King Jr. (≈17,000 pages). Due to a court order, however, some information has been removed and many other pages will not be released until the year 2027.[49]

1967–73: The now-defunct Project MINARET was created to spy on U.S. citizens. At the request of the U.S. Army, those who protested against the Vietnam War were put on the NSA's "watch list".[17]



Church Committee of the United States Senate published the final report on "*Intelligence Activities and the Rights of Americans*" in 1976 (PDF, 26.54 MB)



Walt Disney served as a "S.A.C. Contact" (trusted informant) for the U.S. government to weed out communists and dissidents from the entertainment industry, according to documents obtained by *The New York Times*.^[50]

See also: [Hollywood blacklist](#)

Church committee review

[\[edit\]](#)

1975: The Church Committee of the United States Senate was set up to investigate widespread intelligence abuses by the NSA, CIA and FBI.[12] Domestic surveillance, authorized by the highest executive branch of the federal government, spanned from the FDR Administration to the Presidency of Richard Nixon. The following examples were reported by the Church Committee:

●**President Roosevelt** asked the FBI to put in its files the names of citizens sending telegrams to the White House opposing his "national defense" policy and supporting Col. Charles Lindbergh.[51]

●**President Truman** received inside information on a former Roosevelt aide's efforts to influence his appointments, labor union negotiating plans, and the publishing plans of journalists.[51]

●**President Eisenhower** received reports on purely political and social contacts with foreign officials by Bernard Baruch, Eleanor Roosevelt, and Supreme Court Justice William O. Douglas.[51]

●The **Kennedy administration** ordered the FBI to wiretap a congressional staff member, three executive officials, a lobbyist, and a Washington law firm. US Attorney General Robert F. Kennedy received data from an FBI wire tap on Martin Luther King Jr. and an electronic listening device targeting a congressman, both of which yielded information of a political nature.[51]

●**President Johnson** asked the FBI to conduct "name checks" on his critics and members of the staff of his 1964 opponent, Senator Barry Goldwater. He also requested purely political intelligence on his critics in the Senate, and received extensive intelligence reports on political activity at the 1964 Democratic Convention from FBI electronic surveillance.[51]

●**President Nixon** authorized a program of wiretaps which produced for the White House purely political or personal information unrelated to national security, including information about a Supreme Court justice.[51]

The Final Report (Book II) of the Church Committee revealed the following statistics:

●Over 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a "national emergency".[51]

●Over 500,000 domestic intelligence files were kept at the FBI headquarters, of which 65,000 were opened in 1972 alone.[51]

●At least 130,000 first class letters were opened and photographed by the FBI from 1940 to 1966.[51]

●A quarter of a million first class letters were opened and photographed by the CIA from 1953 to 1973.[51]

●Millions of private telegrams sent from, or to, through the United States were obtained by the National Security Agency (NSA), under a secret arrangement with U.S. telegraph companies, from 1947 to 1975.[51]

●Over 100,000 Americans have been indexed in U.S. Army intelligence files.[51]

- About 300,000 individuals were indexed in a CIA computer system during the course of Operation CHAOS.[51]

- Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service (IRS), with tax investigations "done on the basis of political rather than tax criteria".[51]

In response to the committee's findings, the United States Congress passed the Foreign Intelligence Surveillance Act in 1978, which led to the establishment of the United States Foreign Intelligence Surveillance Court, which was authorized to issue surveillance warrants.[52]

Several decades later in 2013, the presiding judge of the FISA Court, Reggie Walton, told *The Washington Post* that the court only has a limited ability to supervise the government's surveillance, and is therefore "forced" to rely upon the accuracy of the information that is provided by federal agents.[53]

On August 17, 1975 Senator Frank Church stated on NBC's "Meet the Press" without mentioning the name of the NSA about this agency:

In the need to develop a capacity to know what potential enemies are doing, the United States government has perfected a technological capability that enables us to monitor the messages that go through the air. Now, that is necessary and important to the United States as we look abroad at enemies or potential enemies. We must know, at the same time, that capability at any time could be turned around on the American people, and no American would have any privacy left such is the capability to monitor everything — telephone conversations, telegrams, it doesn't matter. There would be no place to hide.

If this government ever became a tyrant, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology.

I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss. That is the abyss from which there is no return.[54][55][56]

ECHELON

[\[edit\]](#)

Main article: ECHELON

In 1988 an article titled "Somebody's listening" by Duncan Campbell in the *New Statesman* described the signals-intelligence gathering activities of a program code-named "ECHELON".^[57] The program was engaged by English-speaking World War II Allied countries – Australia, Canada, New Zealand, the United Kingdom and the United States (collectively known as AUSCANNZUKUS). It was created by the five countries to monitor the military and diplomatic communications of the Soviet Union and of its Eastern Bloc allies during the Cold War in the early 1960s.^[58]

By the 1990s the ECHELON system could intercept satellite transmissions, public switched telephone network (PSTN) communications (including most Internet traffic), and transmissions carried by microwave. The New Zealand journalist Nicky Hager provided a detailed description of ECHELON in his 1996 book *Secret Power*.^[59] While some member governments denied the existence of ECHELON, a report by a committee of the European Parliament in 2001 confirmed the program's use and warned Europeans about its reach and effects.^[60] The European Parliament stated in its report that the term "ECHELON" occurred in a number of contexts, but that the evidence presented indicated it was a signals-intelligence collection system capable of interception and content-inspection of telephone calls, fax, e-mail and other data-traffic globally.^[58]

James Bamford further described the capabilities of ECHELON in *Body of Secrets* (2002) about the National Security Agency.^[61] Intelligence monitoring of citizens, and their communications, in the area covered by the AUSCANNZUKUS security agreement have, over the years, caused considerable public concern.^{[62][63]}

Escalation following September 11, 2001 attacks

[\[edit\]](#)

Further information: NSA warrantless surveillance (2001–07)

We will come together to strengthen our intelligence capabilities to know the plans of terrorists before they act and to find them before they strike.

—President Bush speaking in Congress on September 20, 2001^[64]



September 11 attacks on the World Trade Center and the Pentagon led to major reforms of U.S. intelligence agencies, and paved the way for the establishment



of the [Director of National Intelligence](#) position. *The New York Times* wrote that "*Bush Lets U.S. Spy on Callers Without Courts*,^[65] the President emphasized that "*This is a limited program designed to prevent attacks on the United States of America. And I repeat, limited.*"^[66]

In the aftermath of the September 2001 attacks on the World Trade Center and the Pentagon, bulk domestic spying in the United States increased dramatically. The desire to prevent future attacks of this scale led to the passage of the Patriot Act. Later acts include the Protect America Act (which removes the warrant requirement for government surveillance of foreign targets)^[67] and the FISA Amendments Act (which relaxed some of the original FISA court requirements).

In 2002, "Total Information Awareness" was established by the U.S. government in order to "revolutionize the ability of the United States to detect, classify and identify foreign terrorists".^[68]

In 2005, a report about President Bush's President's Surveillance Program appeared in *The New York Times*. According to reporters James Risen and Eric Lichtblau, the actual publication of their report was delayed for a year because "The White House asked *The New York Times* not to publish this article".^[65]

Also in 2005, the existence of STELLARWIND was revealed by Thomas Tamm.^[69] In 2006, Mark Klein revealed the existence of Room 641A that he had wired back in 2003.^[70] In 2008, Babak Pasdar, a computer security expert, and CEO of Bat Blue publicly revealed the existence of the "Quantico circuit", that he and his team found in 2003. He

described it as a back door to the federal government in the systems of an unnamed wireless provider; the company was later independently identified as Verizon.^[71]

The NSA's database of American's phone calls was made public in 2006 by *USA Today* journalist Leslie Cauley in an article titled, "NSA has massive database of Americans' phone calls."^[72] The article cites anonymous sources that described the program's reach on American citizens:

... it means that the government has detailed records of calls they made — across town or across the country — to family members, co-workers, business contacts and others. The three telecommunications companies are working under contract with the NSA, which launched the program in 2001 shortly after the Sept. 11 terrorist attacks.^[72]

In 2009, *The New York Times* cited several anonymous intelligence officials alleging that "the N.S.A. made Americans targets in eavesdropping operations based on insufficient evidence tying them to terrorism" and "the N.S.A. tried to wiretap a member of Congress without a warrant".^[73]

Acceleration of media leaks (2010–present)

[\[edit\]](#)

On 15 March 2012, the American magazine *Wired* published an article with the headline "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)",^[74] which was later mentioned by U.S. Rep. Hank Johnson during a congressional hearing. In response to Johnson's inquiry, NSA director Keith B. Alexander testified that these allegations made by *Wired* magazine were untrue:

show

Excerpt from *Wired* magazine's article originally published on 15 March 2012^[74]

show

NSA Director Keith Alexander's testimony to the United States Congress on 20 March 2012^[75]

2013 mass surveillance disclosures

[\[edit\]](#)

Main article: 2013 mass surveillance disclosures

Part of a series on

Mass surveillance



By location

- Australia
- Canada
- China
- East Germany
- India
- Iran
- New Zealand
- North Korea
- Russia
- South Africa
- United Kingdom
- **United States**
-

On 6 June 2013, Britain's *The Guardian* newspaper began publishing a series of revelations by an unnamed American whistleblower, revealed several days later to be former CIA and NSA-contracted systems analyst Edward Snowden. Snowden gave a cache of internal documents in support of his claims to two journalists: Glenn Greenwald and Laura Poitras, Greenwald later estimated that the cache contains 15,000–20,000 documents, some very large and very detailed, and some very small.^[76]^[77] This was one of the largest news leaks in the modern history of the United States.^[25] In over two months of publications, it became clear that the NSA operates a complex web of spying programs which allow it to intercept internet and telephone conversations from over a billion users from dozens of countries around the world. Specific revelations have been made about China, the European Union, Latin America, Iran and Pakistan, and Australia and New Zealand, however the published documentation reveals that many of the programs indiscriminately collect bulk information directly from central servers and internet backbones, which almost invariably carry and reroute information from distant countries.

Due to this central server and backbone monitoring, many of the programs overlap and interrelate among one another. These programs are often done with the assistance of US entities such as the United States Department of Justice and the FBI,^[78] are sanctioned by US laws such as the FISA Amendments Act, and the necessary court orders for them are signed by the secret Foreign Intelligence Surveillance Court. In addition to this, many of the NSA's programs are directly aided by national and foreign intelligence services, Britain's GCHQ and Australia's DSD, as well as by large private telecommunications and Internet corporations, such as Verizon, Telstra,^[79] Google and Facebook.^[80]

On 9 June 2013, Edward Snowden told *The Guardian*:

They (the NSA) can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer.

—Edward Snowden^[81]

The US government has aggressively sought to dismiss and challenge Fourth Amendment cases raised: *Hepting v. AT&T*, *Jewel v. NSA*, *Clapper v. Amnesty International*, *Al-Haramain Islamic Foundation v. Obama*, and *Center for Constitutional Rights v. Bush*. The government has also granted retroactive immunity to ISPs and telecoms participating in domestic surveillance.^{[82][83]}

The US district court judge for the District of Columbia, Richard Leon, declared^{[84][85][86][87][88][89]} on December 16, 2013 that the mass collection of metadata of Americans' telephone records by the National Security Agency probably violates the Fourth Amendment prohibition of unreasonable searches and seizures.^[90]

Given the limited record before me at this point in the litigation – most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics – I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.^[91]

"Plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the government's interest in collecting and analysing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the fourth amendment," he wrote.^[91]

"The Fourth Amendment typically requires 'a neutral and detached authority be interposed between the police and the public,' and it is offended by 'general warrants' and laws that allow searches to be conducted 'indiscriminately and without regard to their connections with a crime under investigation,'" he wrote.^[92] He added:

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.^[92]

Leon granted the request for a preliminary injunction that blocks the collection of phone data for two private plaintiffs (Larry Klayman, a conservative lawyer, and Charles Strange, father of a cryptologist killed in Afghanistan when his helicopter was shot down in 2011)^[91] and ordered the government to destroy any of their records that have been gathered. But the judge stayed action on his ruling pending a government appeal, recognizing in his 68-page opinion the "significant national security interests at stake in this case and the novelty of the constitutional issues."^[90]

H.R.4681 – Intelligence Authorization Act for Fiscal Year

2015

[\[edit\]](#)

On 20 May 2014, U.S. Representative for Michigan's 8th congressional district Republican congressman Mike Rogers introduced Intelligence Authorization Act for Fiscal Year 2015 with the goal of authorizing appropriations for fiscal years 2014 and 2015 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency (CIA) Retirement and Disability System, and for other purposes.^[93]

Some of its measures cover the limitation on retention. A covered communication (meaning any nonpublic telephone or electronic communication acquired without the consent of a person who is a party to the communication, including communications in electronic storage) shall not be retained in excess of 5 years, unless: (i) the communication has been affirmatively determined, in whole or in part, to constitute foreign intelligence or counterintelligence or is necessary to understand or assess foreign intelligence or counterintelligence; (ii) the communication is reasonably believed to constitute evidence of a crime and is retained by a law enforcement agency; (iii) the communication is enciphered or reasonably believed to have a secret meaning; (iv) all parties to the communication are reasonably believed to be non-United States persons; (v) retention is necessary to protect against an imminent threat to human life, in which case both the nature of the threat and the information to be retained shall be reported to the congressional intelligence committees not later than 30 days after the date such retention is extended under this clause; (vi) retention is necessary for technical assurance or compliance purposes, including a court order or discovery obligation, in which case access to information retained for technical assurance or compliance purposes shall be reported to the congressional intelligence committees on an annual basis; (vii) retention for a period in excess of 5 years is approved by the head of the element of the intelligence community responsible for such retention, based on a determination that retention is necessary to protect the national security of the United States, in which case the head of such element shall provide to the congressional

intelligence committees a written certification describing (I) the reasons extended retention is necessary to protect the national security of the United States; (II) the duration for which the head of the element is authorizing retention; (III) the particular information to be retained; and (IV) the measures the element of the intelligence community is taking to protect the privacy interests of United States persons or persons located inside the United States.[94]

On 10 December 2014, Republican U.S. Representative for Michigan's 3rd congressional district member of Congress Justin Amash criticized the act on his Facebook as being "one of the most egregious sections of law I've encountered during my time as a representative" and "It grants the executive branch virtually unlimited access to the communications of every American".[95]

USA Freedom Act

[\[edit\]](#)

The USA Freedom Act was signed into law on June 2, 2015, the day after certain provisions of the Patriot Act had expired. It mandated an end to bulk collection of phone call metadata by the NSA within 180 days, but allowed continued mandatory retention of metadata by phone companies with access by the government with case-by-case approval from the Foreign Intelligence Surveillance Court.[96]

Modalities, concepts, and methods

[\[edit\]](#)



[Information Awareness Office](#) – a U.S. agency which developed technologies for mass surveillance

Logging postal mail

[\[edit\]](#)

Main article: Mail Isolation Control and Tracking

Under the Mail Isolation Control and Tracking program, the U.S. Postal Service photographs the exterior of every piece of paper mail that is processed in the United States — about 160 billion pieces in 2012. The U.S. Postmaster General stated that the system is primarily used for mail sorting, but the images are available for possible use by law enforcement agencies.^[97] Created in 2001 following the anthrax attacks that killed five people, it is a sweeping expansion of a 100-year-old program called "mail cover" which targets people suspected of crimes. Together, the two programs show that postal mail is subject to the same kind of scrutiny that the National Security Agency gives to telephone calls, e-mail, and other forms of electronic communication.^[98]

Mail cover surveillance requests are granted for about 30 days, and can be extended for up to 120 days. Images captured under the Mail Isolation Control and Tracking program are retained for a week to 30 days and then destroyed.^[97] There are two kinds of mail covers: those related to criminal activity and those requested to protect national security. Criminal activity requests average 15,000 to 20,000 per year, while the number of requests for national security mail covers has not been made public. Neither the Mail Isolation Control and Tracking program nor the mail cover program require prior approval by a judge. For both programs the information gathered is metadata from the outside of the envelope or package for which courts have said there is no expectation of privacy. Opening the mail to view its contents would require a warrant approved by a judge.^[98]

Wiretapping

[\[edit\]](#)

Billions of dollars per year are spent, by agencies such as the Information Awareness Office, National Security Agency, and the Federal Bureau of Investigation, to develop, purchase, implement, and operate systems such as Carnivore, ECHELON, and NarusInsight to intercept and analyze the immense amount of data that traverses the Internet and telephone system every day.^[99]

The Total Information Awareness program, of the Information Awareness Office, was formed in 2002 by the Pentagon and led by former rear admiral John Poindexter.^[100] The program designed numerous technologies to be used to perform mass surveillance. Examples include advanced speech-to-text programs (so that phone conversations can be monitored en-masse by a computer, instead of requiring human operators to listen to them), social network analysis software to monitor groups of people and their interactions with each other, and "Human identification at a distance" software which allows computers to identify people on surveillance cameras by their facial features and gait (the way they walk). The program was later renamed "Terrorism Information Awareness", after a negative public reaction.

Legal foundations

[\[edit\]](#)

The Communications Assistance for Law Enforcement Act (CALEA), passed in 1994, requires that all U.S. telecommunications companies modify their equipment to allow easy wiretapping of telephone, VoIP, and broadband Internet traffic.^{[101][102][103]}

In 1999 two models of mandatory data retention were suggested for the US. The first model would record the IP address assigned to a customer at a specific time. In the second model, "which is closer to what Europe adopted", telephone numbers dialed, contents of Web pages visited, and recipients of e-mail messages must be retained by the ISP for an unspecified amount of time.^{[104][105]} In 2006 the International Association of Chiefs of Police adopted a resolution calling for a "uniform data retention mandate" for "customer subscriber information and source and destination information."^[106] The U.S. Department of Justice announced in 2011 that criminal investigations "are being frustrated" because no law currently exists to force Internet providers to keep track of what their customers are doing.^[107]

The Electronic Frontier Foundation was involved in a lawsuit (Hepting v. AT&T) against the telecom giant AT&T Inc. for its assistance to the U.S. government in monitoring the communications of millions of American citizens. Recently^[when?] the documents, which were exposed by a whistleblower who had previously worked for AT&T, and showed schematics of the massive data mining system, were made public.^{[108][109]}

Internet communications

[\[edit\]](#)

The FBI developed the computer programs "Magic Lantern" and CIPAV, which it can remotely install on a computer system, in order to monitor a person's computer activity.^[110]

The NSA has been gathering information on financial records, Internet surfing habits, and monitoring e-mails. It has also performed extensive surveillance on social networks such as Facebook.^[111] Recently, Facebook has revealed that, in the last six months of 2012, they handed over the private data of between 18,000 and 19,000 users to law enforcement of all types—including local police and federal agencies, such as the FBI, Federal Marshals and the NSA.^[112] One form of wiretapping utilized by the NSA is RADON, a bi-directional host tap that can inject Ethernet packets onto the same target. It allows bi-directional exploitation of Denied networks using standard on-net tools. The one limitation of RADON is that it is a USB device that requires a physical connection to a laptop or PC to work. RADON was created by a Massachusetts firm called Netragard. Their founder, Adriel Desautels, said about RADON, "it is our 'safe' malware. RADON is

designed to enable us to infect customer systems in a safe and controllable manner. Safe means that every strand is built with an expiration date that, when reached, results in RADON performing an automatic and clean self-removal."^[113]

The NSA is also known to have splitter sites in the United States. Splitter sites are places where a copy of every packet is directed to a secret room where it is analyzed by the Narus STA 6400, a deep packet inspection device.^[114] Although the only known location is at 611 Folsom Street, San Francisco, California, expert analysis of Internet traffic suggests that there are likely several locations throughout the United States.

Advertising data

[\[edit\]](#)

In September 2022 the EFF and AP revealed their investigation into the use of advertising IDs to develop the Fog Reveal database.^{[115][116]} Fog Reveal aggregates location data from mobile applications, which is then supplied as a service to United States law enforcement agencies.

Intelligence apparatus to monitor Americans

[\[edit\]](#)

Since the September 11 attacks, a vast domestic intelligence apparatus has been built to collect information using FBI, local police, state homeland security offices and military criminal investigators. The intelligence apparatus collects, analyzes and stores information about millions of (if not all) American citizens, most of whom have not been accused of any wrongdoing. Every state and local law enforcement agency is to feed information to federal authorities to support the work of the FBI.^[117]

The PRISM special source operation system was enabled by the Protect America Act of 2007 under President Bush and the FISA Amendments Act of 2008, which legally immunized private companies that cooperated voluntarily with US intelligence collection and was renewed by Congress under President Obama in 2012 for five years until December 2017. According to *The Register*, the FISA Amendments Act of 2008 "specifically authorizes intelligence agencies to monitor the phone, email, and other communications of U.S. citizens for up to a week without obtaining a warrant" ^[citation needed] when one of the parties is outside the U.S.

PRISM was first publicly revealed on 6 June 2013, after classified documents about the program were leaked to *The Washington Post* and *The Guardian* by Edward Snowden.

Telephones

[\[edit\]](#)

In early 2006, *USA Today* reported that several major telephone companies were cooperating illegally with the National Security Agency to monitor the phone records of U.S. citizens, and storing them in a large database known as the NSA call database. This report came on the heels of allegations that the U.S. government had been conducting electronic surveillance of domestic telephone calls without warrants.^[118]

Law enforcement and intelligence services in the United States possess technology to remotely activate the microphones in cell phones in order to listen to conversations that take place nearby the person who holds the phone.^{[119][120][121]}

U.S. federal agents regularly use mobile phones to collect location data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily (whether it is being used or not), using a technique known as multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone.^{[122][123]}

In 2013, the existence of the Hemisphere Project, through which AT&T provides call detail records to government agencies, became publicly known.

Infiltration of smartphones

[\[edit\]](#)

As worldwide sales of smartphones began exceeding those of feature phones, the NSA decided to take advantage of the smartphone boom. This is particularly advantageous because the smartphone combines a myriad of data that would interest an intelligence agency, such as social contacts, user behavior, interests, location, photos and credit card numbers and passwords.^[124]

An internal NSA report from 2010 stated that the spread of the smartphone has been occurring "extremely rapidly"—developments that "certainly complicate traditional target analysis."^[124] According to the document, the NSA has set up task forces assigned to several smartphone manufacturers and operating systems, including Apple Inc.'s iPhone and iOS operating system, as well as Google's Android mobile operating system.^[124] Similarly, Britain's GCHQ assigned a team to study and crack the BlackBerry.^[124]

Under the heading "iPhone capability", the document notes that there are smaller NSA programs, known as "scripts", that can perform surveillance on 38 different features of the iPhone 3 and iPhone 4 operating systems. These include the mapping feature, voicemail and photos, as well as Google Earth, Facebook and Yahoo! Messenger.^[124]

Data mining of subpoenaed records

[edit]

See also: Data mining, Information extraction, and Predictive analytics

The FBI collected nearly all hotel, airline, rental car, gift shop, and casino records in Las Vegas during the last two weeks of 2003. The FBI requested all electronic data of hundreds of thousands of people based on a very general lead for the Las Vegas New Year's celebration. The Senior VP of The Mirage went on record with PBS' Frontline describing the first time they were requested to help in the mass collection of personal information.^[126]

Surveillance cameras

[edit]

Wide-area motion imagery (WAMI), also known as wide-area persistent surveillance, is a form of airborne surveillance system that collects pattern-of-life data by recording motion images of an area larger than a city – in sub-meter resolution. This video allows for anyone within the field of regard to be tracked – both live and retroactively, for forensic analysis. The use of sophisticated tracking algorithms applied to the WAMI dataset also enables mass automated geo-location tracking of every vehicle and pedestrian.^[127] WAMI sensors are typically mounted on manned airplanes, drones, blimps and aerostats. WAMI is currently in use on the southern border of the US and in the past has been deployed in Baltimore,^[128] Dayton,^[citation needed] and Compton, California in 2012.^{[129][130][131]} An aerial motion imagery surveillance system was deployed more narrowly in Lancaster, California starting in 2012.^{[130][132][133][134]} WAMI systems such as ARGUS WAMI are capable of live viewing and recording a 68 square mile area with enough detail to view pedestrians and vehicles and generate chronographs.^[citation needed] These WAMI cameras, such as Gorgon Stare, Angelfire, Hiper Stare, Hawkeye and ARGUS,^[135] create airborne video so detailed that pedestrians can be followed across the city through forensic analysis. This allows investigators to rewind and playback the movements of anyone within this 68 square mile area for hours, days or even months at a time depending on the airframe the WAMI sensors are mounted on. JLENS, a surveillance aerostat scheduled for deployment over the east coast of the US, is a form of WAMI that uses sophisticated radar imaging along with electro-optical WAMI sensors to enable mass geo-location tracking of ground vehicles.

There has been some resistance to the domestic deployment of WAMI. Its use in Compton, California was intentionally hidden from the public, including from the mayor, because the sheriff's department believed many people would object to the program.^{[136][131][137][134]} The Compton program was revealed and publicized by the American

Civil Liberties Union,^[138] Teame Zazzu,^[127] and The Center for Investigative Reporting.
[\[131\]](#)[\[130\]](#)[\[139\]](#)

After becoming aware of the deployment of WAMI system in her jurisdiction, Compton Mayor Aja Brown proposed requiring that the public be notified before authorities implement monitoring equipment.^[131]

PeSEAS^[140] and PerMIATE^[141] software automate and record the movement observed in the WAMI video.^[142] This technology uses software to track and record the movements of pedestrians and vehicles using automatic object recognition software across the entire frame, generating "tracklets" or chronographs of every car and pedestrian movements. 24/7 deployment of this technology has been suggested by the DHS on spy blimps such as the recently killed Blue Devil Airship.^[143]

Traffic cameras, which were meant to help enforce traffic laws at intersections, have also sparked some controversy, due to their use by law enforcement agencies for purposes unrelated to traffic violations.^[144] These cameras also work as transit choke-points that allow individuals inside the vehicle to be positively identified and license plate data to be collected and time stamped for cross reference with airborne WAMI such as ARGUS and HAWKEYE used by police and Law Enforcement.^[145]

The Department of Homeland Security is funding networks of surveillance cameras in cities and towns as part of its efforts to combat terrorism.^[146] In February 2009, Cambridge, MA rejected the cameras due to privacy concerns.^[147]

In July 2020, the Electronic Frontier Foundation (EFF) reported that the San Francisco Police Department (SFPD) used a camera network in the city's Business Improvement District amid protests against police violence.^[148] The report claims that the SFPD's usage of the camera network went beyond investigating footage, likening the department's access to real-time video feeds as "indiscriminate surveillance of protestors."^[148]

Surveillance drones

[\[edit\]](#)

On 19 June 2013, FBI Director Robert Mueller told the United States Senate Committee on the Judiciary that the federal government had been employing surveillance drones on U.S. soil in "particular incidents".^[149] According to Mueller, the FBI is currently in the initial stage of developing drone policies.^[149]

Earlier in 2012, Congress passed a US\$63 billion bill that will grant four years of additional funding to the Federal Aviation Administration (FAA). Under the bill, the FAA is required to provide military and commercial drones with expanded access to U.S. airspace by October 2015.^[150]

In February 2013, a spokesman for the Los Angeles Police Department explained that these drones would initially be deployed in large public gatherings, including major protests. Over time, tiny drones would be used to fly inside buildings to track down suspects and assist in investigations.^[151] According to *The Los Angeles Times*, the main advantage of using drones is that they offer "unblinking eye-in-the-sky coverage". They can be modified to carry high-resolution video cameras, infrared sensors, license plate readers, listening devices, and be disguised as sea gulls or other birds to mask themselves.^[151]

The FBI and Customs and Border Protection have used drones for surveillance of protests by the Black Lives Matter movement.^[152]

Infiltration of activist groups

[\[edit\]](#)

In 2003, consent decrees against surveillance around the country were lifted, with the assistance of the Justice Department.^[153]

The New York City Police Department infiltrated and compiled dossiers on protest groups before the 2004 Republican National Convention, leading to over 1,800 arrests and subsequent fingerprinting.^[154]

In 2008, Maryland State Police infiltrated local peace groups.^[155]

In 2013, a Washington, D.C. undercover cop infiltrated peace groups.^[156]

The Intercept claimed that in 2020, the FBI paid an informant to pose as organizer in Denver, Colorado during the George Floyd protests. This informant particularly infiltrated and undermined protest movements by accusing other genuine activists of being FBI informants.^[157]






International cooperation

[\[edit\]](#)





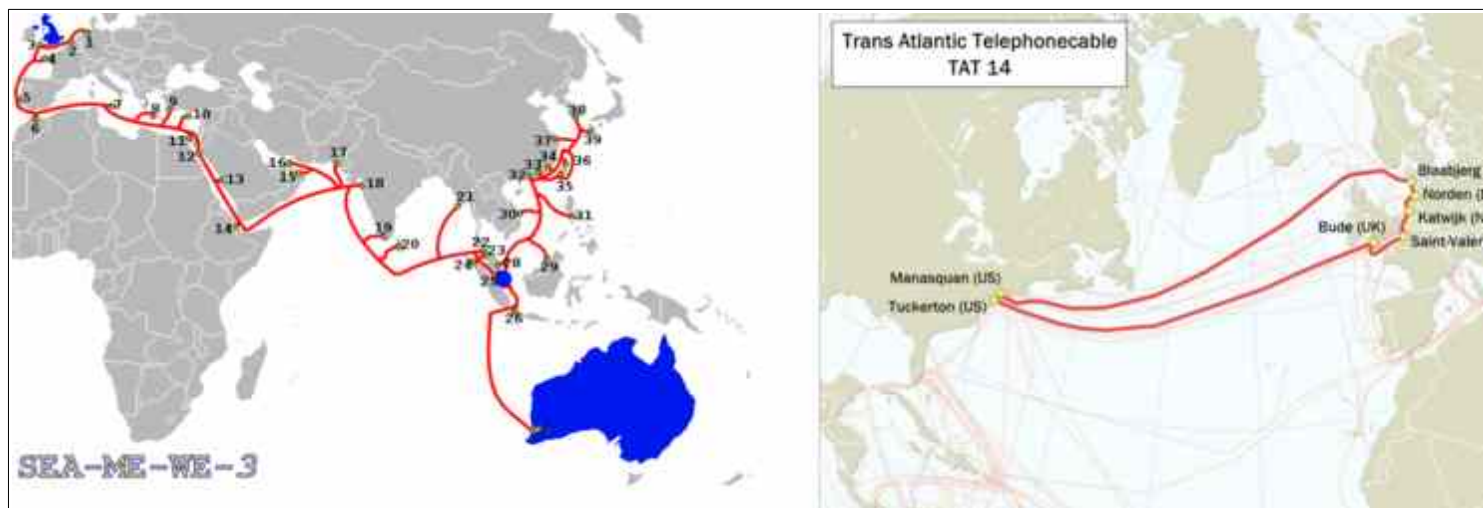
During World War II, the BRUSA Agreement was signed by the governments of the United States and the United Kingdom for the purpose of intelligence sharing. This was later formalized in the UKUSA Agreement of 1946 as a secret treaty. The full text of the agreement was released to the public on 25 June 2010.^[158]

Although the treaty was later revised to include other countries such as Denmark, Germany, Ireland, Norway, Turkey, and the Philippines,^[158] most of the information sharing is performed by the so-called "Five Eyes",^[159] a term referring to the following English-speaking western democracies and their respective intelligence agencies:

-  – The Defence Signals Directorate of Australia^[159]
 -  – The Communications Security Establishment of Canada^[159]
 -  – The Government Communications Security Bureau of New Zealand^[159]
 -  – The Government Communications Headquarters of the United Kingdom, which is widely considered to be a leader in traditional spying due to its influence on countries that were once part of the British Empire.^[159]
 -  – The National Security Agency of the United States, which has the biggest budget and some of the most advanced technical abilities among the "five eyes".^[159]
- In 2013, media disclosures revealed how other government agencies have cooperated extensively with the "Five Eyes":

-  – The Politiets Efterretningstjeneste (PET) of Denmark, a domestic intelligence agency, exchanges data with the NSA on a regular basis, as part of a secret agreement with the United States.^[160]
-  – The Bundesnachrichtendienst (*Federal Intelligence Service*) of Germany systematically transfers metadata from German intelligence sources to the NSA. In December 2012 alone, Germany provided the NSA with 500 million metadata records.^[161] The NSA granted the Bundesnachrichtendienst access to X-Keyscore,^[162] in exchange for Mira4 and Veras.^[161] In early 2013, Hans-Georg Maaßen, President of the German domestic security agency BfV, made several visits to the headquarters of the NSA. According to classified documents of the German government, Maaßen had agreed to transfer all data collected by the BfV via XKeyscore to the NSA.^[163] In addition, the BfV has been working very closely with eight other U.S. government agencies, including the CIA.^[164]
-  – The SIGINT National Unit of Israel routinely receives raw intelligence data (including those of U.S. citizens) from the NSA.^[165] (See also: Memorandum of understanding between the NSA and Israel)
-  – The Algemene Inlichtingen en Veiligheidsdienst (*General Intelligence and Security Service*) of the Netherlands has been receiving and storing user information gathered by U.S. intelligence sources such as PRISM.^[166]
-  – The Defence Ministry of Singapore and its Security and Intelligence Division have been secretly intercepting much of the fibre optic cable traffic passing through the Asian continent. Information gathered by the Government of Singapore is transferred to the Government of Australia as part of an intelligence sharing agreement. This allows the "Five Eyes" to maintain a "stranglehold on communications across the Eastern Hemisphere".^[167]

-  – The National Defence Radio Establishment of Sweden (codenamed Sardines) [168] has been working extensively with the NSA, and it has granted the "five eyes" access to underwater cables in the Baltic Sea.[168]
-  – The Federal Intelligence Service (FSI) of Switzerland regularly exchanges information with the NSA, based on a secret agreement.[160][169] In addition, the NSA has been granted access to Swiss monitoring facilities in Leuk (canton of Valais) and Herrenschwanden (canton of Bern).[160]



Top secret documents leaked by [Edward Snowden](#) revealed that the "Five Eyes" have gained access to the majority of Internet and telephone communications flowing throughout Europe, the United States, and other parts of the world.

Left: [SEA-ME-WE 3](#), which runs across the [Afro-Eurasian supercontinent](#) from Japan to [Northern Germany](#), is one of the most important [submarine cables](#) accessed by the "Five Eyes". Singapore, a former British colony in the Asia-Pacific region (blue dot), plays a vital role in intercepting Internet and telecommunications traffic heading from Australia/Japan to Europe, and vice versa. An intelligence sharing agreement between Singapore and Australia allows the rest of the "Five Eyes" to gain access to [SEA-ME-WE 3](#).^[167]

Right: [TAT-14](#), a telecommunications cable linking Europe with the United States, was identified as one of few assets of "Critical Infrastructure and Key Resources" of the USA on foreign territory. In 2013, it was revealed that British officials "pressured a handful of telecommunications and internet companies" to allow the British government to gain access to [TAT-14](#).^[170]

Aside from the "Five Eyes", most other Western countries are also participating in the NSA surveillance system and sharing information with each other.^[171] However, being a partner of the NSA does not automatically exempt a country from being targeted by the NSA. According to an internal NSA document leaked by Snowden, "We (the NSA) can, and often do, target the signals of most 3rd party foreign partners."^[172]

Examples of members of the "Five Eyes" spying for each other:

- On behalf of the British Prime Minister Margaret Thatcher, the Security Intelligence Service of Canada spied on two British cabinet ministers in 1983.^[173]
- The U.S. National Security Agency spied on and intercepted the phone calls of Princess Diana right until she died in a Paris car crash with Dodi Fayed in 1997. The NSA currently

holds 1,056 pages of classified information about Princess Diana, which cannot be released to the public because their disclosure is expected to cause "*exceptionally grave damage*" to the national security of the United States.[174]

Uses of intercepted data

[\[edit\]](#)

Most of the NSA's collected data which was seen by human eyes (i.e., used by NSA operatives) was used in accordance with the stated objective of combating terrorism.
[\[175\]](#)[\[176\]](#)[\[177\]](#)

In addition to combatting terrorism, these surveillance programs have been employed to assess the foreign policy and economic stability of other countries.[178]

According to reports by Brazil's O Globo newspaper, the collected data was also used to target "commercial secrets".[179] In a statement addressed to the National Congress of Brazil, journalist Glenn Greenwald testified that the U.S. government uses counter-terrorism as a "pretext" for clandestine surveillance in order to compete with other countries in the "business, industrial and economic fields".[\[180\]](#)[\[181\]](#)

In an interview with *Der Spiegel* published on 12 August 2013, former NSA Director Michael Hayden admitted that "We [the NSA] steal secrets. We're number one in it". Hayden also added that "We steal stuff to make you safe, not to make you rich".[178]

According to documents seen by the news agency Reuters, information obtained in this way is subsequently funnelled to authorities across the nation to help them launch criminal investigations of Americans.[182] Federal agents are then instructed to "recreate" the investigative trail in order to "cover up" where the information originated, [182] known as parallel construction. (Were the true origins known, the evidence and resulting case might be invalidated as "fruit of the poisonous tree", a legal doctrine designed to deter abuse of power that prevents evidence or subsequent events being used in a case if they resulted from a search or other process that does not conform to legal requirements.)

According to NSA Chief Compliance Officer John DeLong, most violations of the NSA's rules were self-reported, and most often involved spying on personal love interests using surveillance technology of the agency.[183]

Most agricultural surveillance is not covert and is carried out by government agencies such as APHIS (USDA's Animal and Plant Health Inspection Service).[184] DHS has lamented the limited surveillance coverage provided by these inspections and works to augment this protection with their own resources.[184]

See also

[\[edit\]](#)

- Censorship in the United States
- Domain Awareness System
- Freedom of speech in the United States
- Global surveillance
- Internet censorship in the United States
- Labor spying in the United States
- List of Americans under surveillance
- List of government mass surveillance projects
- Mass surveillance in the United Kingdom
- Police surveillance in New York City

References

[\[edit\]](#)

- ¹ ^ Farrell, Paul (2 December 2013). "History of 5-Eyes – explainer". *The Guardian*. Retrieved 14 October 2017.
- ² ^ "Unmasking the Five Eyes' global surveillance practices - GISWatch". *giswatch.org*. Retrieved 14 October 2017.
- ³ ^ "Obama quietly extends post-9/11 state of national emergency". *Msnbc.com*. 11 September 2013. Retrieved 14 October 2017.
- ⁴ ^ House, The White (10 September 2024). "Message to the Congress on the Continuation of the National Emergency With Respect to Certain Terrorist Attacks". *The White House*. Retrieved 11 November 2024.
- ⁵ ^ "The New Political Prisoners: Leakers, Hackers and Activists". *Rolling Stone*. March 2013. Retrieved 14 October 2017.
- ⁶ ^ "Exclusive: Inside the Army Spy Ring & Attempted Entrapment of Peace Activists, Iraq Vets, Anarchists". *Democracynow.org*. Retrieved 14 October 2017.
- ⁷ ^ "The FBI vs. Occupy: Secret Docs Reveal 'Counterterrorism' Monitoring of OWS from Its Earliest Days". *Democracynow.org*. Retrieved 14 October 2017.
- ⁸ ^ Jump up to:^a ^b Glenn Greenwald (31 July 2013). "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'". *The Guardian*. Retrieved 2 August 2013.
- ⁹ ^ Mui, Yan (29 July 2013). "Growing use of FBI screens raises concerns about accuracy, racial bias". *The Washington Post*. Retrieved 2 August 2013.
- ¹⁰ ^ Winston, Ali (11 August 2016). "Marked for Life: U.S. Government Using Gang Databases to Deport Undocumented Immigrants". *The Intercept*. Retrieved 14 October 2017.
- ¹¹ ^ "Pre-1952 Historical Timeline". NSA. Retrieved 6 November 2017.

- 12.^ Jump up to:[a](#) [b](#) [c](#) [d](#) [e](#) [f](#) "Factbox: History of mass surveillance in the United States". Reuters. 7 June 2013. Retrieved 14 August 2013.
- 13.^ "Hall of Honor 1999 Inductee – Herbert O. Yardley". NSA.
- 14.^ Jump up to:[a](#) [b](#) "Return to Sender: U.S. Censorship of Enemy Alien Mail in World War II", Louis Fiset, *Prologue Magazine*, Vol. 33, No. 1 (Spring 2001). Retrieved 5 October 2013.
- 15.^ Kennett, Lee (1985). *For the duration... : the United States goes to war, Pearl Harbor-1942*. New York: Scribner. ISBN .
- 16.^ The Center for Cryptologic History. "The Origins of NSA (NSA.gov)". Archived from the original on 18 March 2004.
- 17.^ Jump up to:[a](#) [b](#) [c](#) Epsley-Jones, Katelyn; Frenzel, Christina. "The Church Committee Hearings & the FISA Court". PBS. Retrieved 14 August 2013.
- 18.^ Truman, Harry S. (24 October 1952). "Memorandum" (PDF). *National Security Agency*.
- 19.^ Gearan, Anne (6 June 2013). "'No Such Agency' spies on the communications of the world". *Washington Post*. ISSN 0190-8286. Retrieved 6 November 2017.
- 20.^ "TAP: Vol 12, Iss. 19. Back to Church. Chris Mooney". 5 December 2006. Archived from the original on 5 December 2006. Retrieved 6 November 2017.
- 21.^ "NSA inspector general report on email and internet data collection under Stellar Wind – full document". *the Guardian*. 27 June 2013. Retrieved 6 November 2017.
- 22.^ "The New York Times" (PDF).
- 23.^ Poitras, Laura; Greenwald, Glenn (9 June 2013). "NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video". *The Guardian*. ISSN 0261-3077. Retrieved 20 November 2017.
- 24.^ Jump up to:[a](#) [b](#) Gellman, Barton; Poitras, Laura (7 June 2013). "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program". *The Washington Post*. ISSN 0190-8286. Retrieved 6 November 2017.
- 25.^ Jump up to:[a](#) [b](#) "Ex-CIA employee source of leak on PRISM program". France 24. 9 June 2013. Retrieved 17 September 2013. Snowden's decision to reveal his identity and whereabouts lifts the lid on one of the biggest security leaks in US history and escalates a story that has placed a bright light on Obama's extensive use of secret surveillance.
- 26.^ "The NSA and the NSC, any connection? - Democratic Underground". Archived from the original on 17 August 2016. Retrieved 9 August 2016.
- 27.^ "National Security Council". *The White House*. Retrieved 25 September 2023.
- 28.^ "The National Security Agency is established, Nov. 4, 1952". *Politico.com*. 4 November 2010. Retrieved 14 October 2017.
- 29.^ Bamford, James (25 December 2005). "The Agency That Could Be Big Brother". *The New York Times*. Retrieved 14 August 2013.
- 30.^ DAVID BURNHAM (1 February 1986). "TRUMAN WIRETAPS ON EX-NEW DEAL AIDE CITED". *The New York Times*. Retrieved 18 September 2013.
- 31.^ Jump up to:[a](#) [b](#) Gentry, C. (2001). *J. Edgar Hoover: The Man and the Secrets*. W. W. Norton. ISBN .
- 32.^ Wolf, Paul (9 March 2016). *COINTELPRO: The Untold American Story* (PDF).
- 33.^ "Question: Why is Eleanor Roosevelt's FBI file so large?". George Washington University. Retrieved 18 September 2013.

- 34.^ "Eleanor Roosevelt". History (U.S. TV channel). Retrieved 18 September 2013. J. Edgar Hoover (1895–1972), the longtime director of the Federal Bureau of Investigation, considered Eleanor Roosevelt's liberal views dangerous and believed she might be involved in communist activities. He ordered his agents to monitor Roosevelt and keep what became an extensive file on her.
- 35.^ RONALD J. OSTROW & LISA GETTER (9 December 1998). "FBI Files on Sinatra Detail Links to JFK, Mob Figures". *Los Angeles Times*. Retrieved 18 September 2013.
- 36.^ MOLOTSKY, IRVIN (9 December 1998). "F.B.I. Releases Its Sinatra File, With Tidbits Old and New". *The New York Times*. Retrieved 18 September 2013.
- 37.^ Jump up to:^a ^b "FBI removes many redactions in Marilyn Monroe file". Associated Press. Archived from the original on 27 September 2013. Retrieved 18 September 2013.
- 38.^ Jump up to:^a ^b Cohen, Adam (21 September 2006). "While Nixon Campaigned, the F.B.I. Watched John Lennon". *The New York Times*. Retrieved 18 September 2013.
- 39.^ Gumbel, Andrew. "The Lennon Files: The FBI and the Beatle". *The Independent*. London. Archived from the original on 4 October 2015. Retrieved 18 September 2013.
- 40.^ Laurent Belsie. "US hoped to deport John Lennon". *The Christian Science Monitor*. Retrieved 18 September 2013.
- 41.^ Overbye, Dennis (7 May 2002). "New Details Emerge From the Einstein Files; How the F.B.I. Tracked His Phone Calls and His Trash". *The New York Times*. Retrieved 17 September 2013.
- 42.^ "FBI campaign against Einstein revealed". BBC. 8 June 2002. Retrieved 17 September 2013.
- 43.^ "Albert Einstein: Fact or Fiction?". History (U.S. TV channel). Retrieved 17 September 2013. Because of his controversial political beliefs-his support for socialism, civil rights, and nuclear disarmament, for example-many anti-Communist crusaders believed that Einstein was a dangerous subversive. Some, like FBI director J. Edgar Hoover, even thought he was a spy. For 22 years, Hoover's agents tapped Einstein's phones, opened his mail, rifled through his trash and even bugged his secretary's nephew's house, all to prove that he was more radical (as his 1,500-page FBI dossier noted) than "even Stalin himself."
- 44.^ Church, Frank (23 April 1976). Church Committee Book III. *Dr. Martin Luther King, Jr., Case Study* (Report). Church Committee.
- 45.^ Jump up to:^a ^b "FBI tracked King's every move". CNN. 29 December 2008. Retrieved 17 September 2013.
- 46.^ "'Life Lessons' From a White House Plumber". *NPR.org*. NPR. When Daniel Ellsberg leaked the Pentagon Papers to The New York Times in 1971, the Nixon White House tried to discredit him. Among other things, Nixon loyalists burglarized the office of Ellsberg's psychiatrist.
- 47.^ "The Watergate Story". *The Washington Post*. Retrieved 17 September 2013. The White House "plumbers" unit – named for their orders to plug leaks in the administration – burglarizes a psychiatrist's office to find files on Daniel Ellsberg, the former defense analyst who leaked the Pentagon Papers.
- 48.^ "Watergate and the Constitution". National Archives and Records Administration. Retrieved 17 September 2013.
- 49.^ "Martin Luther King, Jr. FBI File". Pickler Memorial Library (Truman State University). Archived from the original on 5 May 2021. Retrieved 17 September 2013.

50. ^ MITGANG, HERBERT (6 May 1993). "Disney Link To the F.B.I. And Hoover Is Disclosed". *The New York Times*. Retrieved 19 September 2013.
51. ^ Jump up to:[a](#) [b](#) [c](#) [d](#) [e](#) [f](#) [g](#) [h](#) [i](#) [j](#) [k](#) [l](#) [m](#) [n](#) Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee"). *Book II, Intelligence Activities and the Rights of Americans* (PDF) (Final Report, S. Rep. No. 94-755 (1976) ed.). United States Senate Select Committee on Intelligence. Archived from the original (PDF) on 21 May 2013.
52. ^ "FISA Court Has Approved Majority of Surveillance Warrants". *Npr.org*. 10 June 2013. Retrieved 14 August 2013.
53. ^ Leonnig, Carol D. (16 August 2013). "Court: Ability to police U.S. spying program limited". *The Washington Post*. Retrieved 16 August 2013.
54. ^ Popkey, Dan (5 August 2013). "Idaho's Frank Church has posthumous TV debate with Rick Santorum". *Idaho Statesman*. Retrieved 21 September 2013.
55. ^ "Sen. Frank Church Warns of How Easily Government Can Abuse Expanding Surveillance Capabilities". *Grabien - The Multimedia Marketplace*. 17 August 1975. Retrieved 21 September 2013.
56. ^ Bamford, James (13 September 2011). "Post-September 11, NSA 'enemies' include us". *Politico*. Retrieved 21 September 2013.
57. ^ Campbell, Duncan (12 August 1988). "Somebody's Listening". *New Statesman*. Archived from the original on 3 January 2007. Retrieved 16 September 2013.
58. ^ Jump up to:[a](#) [b](#) Schmid, Gerhard (11 July 2001). "On the existence of a global system for the interception of private and commercial communications (ECHELON interception system), (2001/2098(INI))" (pdf). European Parliament: Temporary Committee on the ECHELON Interception System. p. 194. Retrieved 16 September 2013.
59. ^ Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network* (1996).
60. ^ Fiddler, Stephen (1 July 2013). Echoes of Echelon in Charges of NSA Spying in Europe. *The Washington Post*.
61. ^ Bamford, James; *Body of Secrets*, Anchor, ISBN 0-385-49908-6; 2002
62. ^ American Civil Liberties (1 May 2000). Privacy Advocates Concerned About Echelon.
63. ^ "Edward Snowden and The Five Eyes - Some guys blog". *Suhailpatel.co.uk*. 26 June 2013. Archived from the original on 22 February 2020. Retrieved 14 October 2017.
64. ^ "Text: President Bush Addresses the Nation". *The Washington Post*. 20 September 2001.
65. ^ Jump up to:[a](#) [b](#) Risen, James; Lichtblau, Eric (16 December 2005). "Bush Lets U.S. Spy on Callers Without Courts". *The New York Times*. Retrieved 14 August 2013. The White House asked *The New York Times* not to publish this article
66. ^ "President Visits Troops at Brooke Army Medical Center". *whitehouse.gov*. 1 January 2006. Retrieved 15 August 2013 – via National Archives.
67. ^ "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II): Hearing Before the H. Comm. on the Judiciary, 110th Cong. 13–30 (statement of J.M. McConnell, Director of National Intelligence)" (PDF). 18 September 2007.
68. ^ Rosen, Jeffrey (15 December 2002). "Total Information Awareness". *The New York Times*. Retrieved 14 August 2013.

- 69.^ Brenner, Joel (2017). "A Review of "The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age" by Laura K. Donohue". *Journal of National Security Law & Policy*. **9**: 1–22. ProQuest 2095680872 – via ProQuest.
- 70.^ "AT&T Whistle-Blower's Evidence". *Wired*. 17 May 2006. Retrieved 14 August 2013.
- 71.^ Poulsen, Kevin (6 March 2008). "Whistle-Blower: Feds Have a Backdoor Into Wireless Carrier — Congress Reacts". *Wired*. Retrieved 14 August 2013.
- 72.^ Jump up to:^a ^b Cauley, Leslie (11 May 2006). "NSA has massive database of Americans' phone calls". *USA Today*. Archived from the original on 13 July 2013.
- 73.^ Lichtblau, Eric; Risen, James (16 April 2009). "Officials Say U.S. Wiretaps Exceeded Law". *The New York Times*. Retrieved 16 August 2013.
- 74.^ Jump up to:^a ^b ^c Bamford, James (15 March 2012). "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". *Wired*. Retrieved 14 August 2013.
- 75.^ Jump up to:^a ^b Greenberg, Andy. "NSA Chief Denies Wired's Domestic Spying Story (Fourteen Times) In Congressional Hearing". *Forbes*. Retrieved 14 August 2013.
- 76.^ Duran-Sanchez, Mabel (10 August 2013). "Greenwald Testifies to Brazilian Senate about NSA Espionage Targeting Brazil and Latin America". Archived from the original on 20 April 2015. Retrieved 13 August 2013.
- 77.^ "Glenn Greenwald afirma que documentos dizem respeito à interesses comerciais do governo americano". 6 August 2013. Retrieved 13 August 2013.
- 78.^ How Microsoft handed the NSA access to encrypted messages, *The Guardian*, 12 July 2013. Retrieved 13 July 2013.
- 79.^ Bridie Jabour in Sydney (12 July 2013). "Telstra signed deal that would have allowed US spying". *The Guardian*. London.
- 80.^ The first three days of revelations were: the FISC court order that Verizon provide bulk metadata on its customers to the NSA; presentation slides explaining the cooperation of nine US Internet giants through the PRISM program; and the bulk collection of Chinese users' text messages, which coincided with Xi Jinping's visit to California to meet Barack Obama.
- 81.^ "NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video". *The Guardian*. Retrieved 17 September 2013.
- 82.^ "Senate caves, votes to give telecoms retroactive immunity". *Ars Technica*. 13 February 2008. Retrieved 16 September 2013.
- 83.^ "Forget Retroactive Immunity, FISA Bill is also about Prospective Immunity". *The Progressive*. 10 July 2008. Archived from the original on 18 September 2013. Retrieved 16 September 2013.
- 84.^ Leon, Richard (16 December 2013). "Federal judge rules NSA program is likely unconstitutional a.k.a. Klayman et al. v. Obama et al. Memorandum and Opinion from December 16, 2013 in Civil Action 13-0851 in United Case District Court for the District of Columbia". *The Washington Post*. Archived from the original on 30 August 2017. Retrieved 17 December 2013.
- 85.^ Savage, Charlie (16 December 2013). "Judge Questions Legality of N.S.A. Phone Records". *The New York Times*. Retrieved 18 December 2013.
- 86.^ Mears, Bill; Perez, Evan (17 December 2013). "Judge: NSA domestic phone data-mining unconstitutional". *CNN*. Retrieved 18 December 2013.

- 87.^ Kravets, David (16 December 2013). "Court Says NSA Bulk Telephone Spying Is Unconstitutional". *Wired*. Retrieved 18 December 2013.
- 88.^ Kevin Johnson & Richard Wolf (16 December 2013). "Federal judge rules against NSA spying". *USA Today*. Retrieved 18 December 2013.
- 89.^ Gerstein, Josh (16 December 2013). "Judge: NSA phone program likely unconstitutional". *Politico*. Retrieved 18 December 2013.
- 90.^ Jump up to:^a ^b Ellen Nakashima & Ann E. Marimow (16 December 2013). "Judge: NSA's collecting of phone records is probably unconstitutional". *The Washington Post*. Retrieved 17 December 2013.
- 91.^ Jump up to:^a ^b ^c Spencer Ackerman & Dan Roberts (16 December 2013). "NSA phone surveillance program likely unconstitutional, federal judge rules". *The Guardian*. Retrieved 18 December 2013.
- 92.^ Jump up to:^a ^b Jake Gibson (17 December 2013). "Judge deals blow to NSA phone data program". Fox News. Retrieved 18 December 2013.
- 93.^ Feinstein, Dianne (7 July 2014). "S.1681 - 113th Congress (2013-2014): Intelligence Authorization Act for Fiscal Year 2014". *www.congress.gov*. Retrieved 7 November 2020.
- 94.^ "H.R.4681 - Intelligence Authorization Act for Fiscal Year 2015". *Congress.gov*. 19 December 2014. Retrieved 14 October 2017.
- 95.^ "Log In or Sign Up to View". *Facebook.com*. Retrieved 14 October 2017.
- 96.^ Peralta, Eyder (29 November 2015). "NSA Ends Sept. 11-Era Surveillance Program". *Npr.org*. Retrieved 14 October 2017.
- 97.^ Jump up to:^a ^b "AP Interview: USPS takes photos of all mail" Archived 2013-08-24 at the Wayback Machine, Associated Press (AP), 2 August 2013.
- 98.^ Jump up to:^a ^b "U.S. Postal Service Logging All Mail for Law Enforcement", Ron Nixon, *New York Times*, July 3, 2013. Retrieved 25 September 2013.
- 99.^ McCullagh, Declan (30 January 2007). "FBI turns to broad new wiretap method". *ZDNet News*. Retrieved 13 March 2009.
- 100.^ Bamford, James (25 December 2005). "The Agency That Could Be Big Brother". *The New York Times*.
- 101.^ "CALEA Archive". Electronic Frontier Foundation. Archived from the original on 3 May 2009. Retrieved 14 March 2009.
- 102.^ "CALEA: The Perils of Wiretapping the Internet". Electronic Frontier Foundation. Retrieved 14 March 2009.
- 103.^ "FAQ on the CALEA Expansion by the FCC". Electronic Frontier Foundation. 20 September 2007. Retrieved 14 March 2009.
- 104.^ Declan McCullagh (14 April 2006). "ISP snooping gaining support". *CNET*. CBS Interactive. Retrieved 17 March 2009.
- 105.^ Declan McCullagh (23 April 2008). "FBI, politicians renew push for ISP data retention laws". *CNET*. CBS Interactive. Retrieved 17 March 2009. Based on the statements at Wednesday's hearing and previous calls for new laws in this area, the scope of a mandatory data retention law remains fuzzy. It could mean forcing companies to store data for two years about what Internet addresses are assigned to which customers (Comcast said in 2006 that it would be retaining those records for six months).
- 106.^ Declan McCullagh (24 January 2011). "GOP pushing for ISPs to record user data". *CNET*. CBS Interactive. Retrieved 27 January 2011.

- 107.^ Declan McCullagh (24 January 2011). "Justice Department seeks mandatory data retention". *CNET*. CBS Interactive. Retrieved 27 January 2011.
- 108.^ "Hepting v. AT&T: Unsealed Klein exhibits", Electronic Frontier Foundation. Retrieved 19 September 2013.
- 109.^ "Secret Surveillance Evidence Unsealed in AT&T Spying Case", Electronic Frontier Foundation, 12 June 2007. Retrieved 19 September 2013.
- 110.^ Kevin Poulsen (18 July 2007). "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats". *Wired Magazine*. Condé Nast. Retrieved 19 September 2013.
- 111.^ "FAQ: What You Need to Know About the NSA's Surveillance Programs — ProPublica". *ProPublica*. 5 August 2013.
- 112.^ "FAQ: What You Need to Know About the NSA's Surveillance Programs". 5 August 2013. Retrieved 7 October 2015.
- 113.^ "The 3 ways we owned you in 2012". *Netragard*. 12 February 2013. Retrieved 12 March 2022.
- 114.^ Clement, Andrew; Obar, Jonathon (2015). "Canadian Internet "Boomerang" Traffic and Mass NSA Surveillance". *Canadian Internet "Boomerang" Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges*. University of Ottawa Press. pp. 17–20. doi:10.2307/j.ctt15nmj3c.5. JSTOR j.ctt15nmj3c.5.
- 115.^ Greenberg, Will (31 August 2022). "Fog Revealed: A Guided Tour of How Cops Can Browse Your Location Data". *Electronic Frontier Foundation*.
- 116.^ Burke, Garance; Dearen, Jason (1 September 2022). "Tech tool offers police 'mass surveillance on a budget'". *AP News*.
- 117.^ Data Priest & William M. Arkin (20 December 2010). "Monitoring America". *Top Secret America, A Washington Post Investigation*. Retrieved 27 January 2011.
- 118.^ Cauley, Leslie (11 May 2006). "NSA has massive database of Americans' phone calls". *USA Today*. Retrieved 12 May 2010.
- 119.^ "FBI using cell phone microphones to eavesdrop", Eric Bangeman, *Ars Technica*, 4 December 2006. Retrieved 17 September 2013.
- 120.^ McCullagh, Declan; Anne Broache (1 December 2006). "FBI taps cell phone mic as eavesdropping tool". *CNet News*. CBS Interactive. Archived from the original on 10 November 2013. Retrieved 14 March 2009.
- 121.^ "Researchers Find Clues in Malware", Nicole Perlroth, *New York Times*, 30 May 2012. Retrieved 20 September 2013.
- 122.^ "Tracking a suspect by mobile phone". *BBC News*. 3 August 2005. Retrieved 14 March 2009.
- 123.^ Miller, Joshua (18 March 2009). "Cell Phone Tracking Can Locate Terrorists – But Only Where It's Legal". *FOX News*. Archived from the original on 18 March 2009. Retrieved 14 March 2009.
- 124.^ Jump up to:**a b c d e** Laura Poitras, Marcel Rosenbach & Holger Stark. "iSpy: How the NSA Accesses Smartphone Data". *Der Spiegel*. Retrieved 9 September 2013.
- 125.^ Laura Poitras; Marcel Rosenbach & Holger Stark. "Photo Gallery: Spying on Smartphones". *Der Spiegel*. Retrieved 9 September 2013.
- 126.^ "Spying on the home front", transcript, FRONTLINE (WGBH Boston), 15 May 2007. Retrieved 19 September 2013.

- 127.^ Jump up to:[a](#) [b](#) Teame Zazzu (31 December 2013). *Stop Wide Area Persistent Surveillance of the USA! Join Teame Zazzu* (Video) – via YouTube.
- 128.^ Internet Society North America Bureau (16 June 2014). "CFP 2014: Persistent Aerial Surveillance". YouTube.
- 129.^ "Sheriff ran air surveillance over Compton without telling residents". *Los Angeles Times*. 23 April 2014. Retrieved 11 December 2024.
- 130.^ Jump up to:[a](#) [b](#) [c](#) Jennings, Angel; Winton, Richard; Rainey, James; Hennigan, W. J. (24 April 2014). "L.A. County Sheriff's Dept. used spy plane to watch Compton". *Los Angeles Times*. Retrieved 11 December 2024.
- 131.^ Jump up to:[a](#) [b](#) [c](#) [d](#) Jennings, Angel; Winton, Richard; Rainey, James (24 April 2014). "Sheriff's secret air surveillance of Compton sparks outrage". *Los Angeles Times*. Retrieved 11 December 2024.
- 132.^ Sewell, Abby; Winton, Richard (25 August 2012). "Lancaster takes to the skies to get a view on crime". *Los Angeles Times*. Retrieved 11 December 2024.
- 133.^ Dilworth, Makeda (23 August 2012). "'Eye in the Sky' takes off". *The Antelope Valley Times*. Palmdale, California: The Antelope Valley Times LLC. Archived from the original on 25 August 2012.
- 134.^ Jump up to:[a](#) [b](#) Cushing, Time (12 May 2014). "Lancaster, California Rolls Out Law Enforcement Surveillance Tech The Right Way". *Techdirt*. Retrieved 11 December 2024.
- 135.^ "Autonomous Real-time Ground Ubiquitous Surveillance – Imaging System (ARGUS-IS)". Archived from the original on 31 January 2010. Retrieved 21 September 2013., Information Processing Processing Techniques Office, U.S. Defense Advanced Research Projects Agency (DARPA). Retrieved 19 September 2013.
- 136.^ Schulz & Pike 2014: "'The system was kind of kept confidential from everybody in the public,' [Compton WAMI project supervisor and L.A. County sheriff's sergeant Doug] Iketani said. 'A lot of people do have a problem with the eye in the sky, the Big Brother, so in order to mitigate any of those kinds of complaints, we basically kept it pretty hush-hush.'"
- 137.^ Cushing, Time (17 April 2014). "LA Sheriff's Dept. On New Surveillance Program: We Knew The Public Wouldn't Like It, So We Kept It A Secret". *Techdirt*. Retrieved 11 December 2024.
- 138.^ "Persistent Aerial Surveillance: Do We Want To Go There, America?". *American Civil Liberties Union*. 7 February 2014.
- 139.^ Schulz, G. W.; Pike, Amanda (11 April 2014). "Hollywood-style surveillance technology inches closer to reality". *cironline.org*. Emeryville, California: The Center for Investigative Reporting. Archived from the original on 13 April 2014.
- 140.^ "DARPA-BAA-09-55: Persistent Stare Exploitation and Analysis System (PerSEAS)", U.S. Defense Advanced Research Projects Agency (DARPA), 18 September 2009. Retrieved 18 September 2013.
- 141.^ "Kitware to develop advanced video analysis workstation as part of DARPA persistent surveillance program", John Keller (ed), Military and Aerospace Electronics, 5 July 2010. Retrieved 19 September 2013.
- 142.^ "Wide Area Airborn [sic] Surveillance: Opportunities and Challenges" on YouTube, Gerard Medioni, University of Southern California, YouTube video, 15 August 2011. Retrieved 9 September 2013.
- 143.^ "Here's the Plan to Fly Missile-Packed Blimps Over Your Home", David Axe, *Wired*, 3 May 2012. Retrieved 9 September 2013.

- 144.^ Erin Mahoney & Joanne Helperin (3 July 2009). "Caught! Big Brother May Be Watching You With Traffic Cameras". Edmunds. Retrieved 19 September 2013.
- 145.^ "Law Enforcement Operations" Archived 2014-05-04 at the Wayback Machine, Persistent Surveillance Systems. Retrieved 9 September 2013.
- 146.^ Savage, Charlie (12 August 2007). "US doles out millions for street cameras". *The Boston Globe*. Retrieved 19 September 2013.
- 147.^ "Cambridge rejects surveillance cameras". *The Boston Globe*. 3 February 2009. Archived from the original on 21 September 2013. Retrieved 19 September 2013.
- 148.^ Jump up to:[a](#) [b](#) Guariglia, Dave Maass and Matthew (27 July 2020). "San Francisco Police Accessed Business District Camera Network to Spy on Protestors". *Electronic Frontier Foundation*. Retrieved 20 October 2020.
- 149.^ Jump up to:[a](#) [b](#) "Mueller: FBI uses drones for surveillance over US soil". BBC. 19 June 2013. Retrieved 24 September 2013.
- 150.^ Kashmir Hill (7 February 2012). "Congress Welcomes The Drones". *Forbes*. Retrieved 24 September 2013.
- 151.^ Jump up to:[a](#) [b](#) rian Bennett & Joel Rubin (15 February 2013). "Drones are taking to the skies in the U.S." *Los Angeles Times*. Retrieved 24 September 2013.
- 152.^ Customs and Border Protection Is Flying a Predator Drone Over Minneapolis - Jason Koebler, Joseph Cox and Jordan Pearson, Motherboard / Vice, 29 May 2020
- 153.^ Cosgrove-Mather, Bootie (6 April 2003). "U.S. Police Surveillance Questioned". *CBS News*. Retrieved 31 January 2014.
- 154.^ McFadden, Robert D. (7 August 2007). "City Is Rebuffed on the Release of '04 Records – New York Times". *New York Times*. Retrieved 5 April 2010.
- 155.^ "Maryland State Police Surveillance of Advocacy Groups Exposed". Center for Effective Government.
- 156.^ Peter Hermann (7 August 2013). "Protesters out undercover officer, accuses her of infiltrating group". *The Washington Post*.
- 157.^ Aaronson, Trevor (7 February 2023). "The FBI Paid a Violent Felon to Infiltrate Denver's Racial Justice Movement". *The Intercept*. Retrieved 6 July 2023.
- 158.^ Jump up to:[a](#) [b](#) Norton-Taylor, Richard (25 June 2010). "Not so secret: deal at the heart of UK-US intelligence". *The Guardian*. London. Retrieved 25 June 2010.
- 159.^ Jump up to:[a](#) [b](#) [c](#) [d](#) [e](#) [f](#) "5-nation spy alliance too vital for leaks to harm". Associated Press. Archived from the original on 25 May 2015. Retrieved 29 August 2013.
- 160.^ Jump up to:[a](#) [b](#) [c](#) "NDB und NSA kooperieren enger als bisher bekannt" (in German). *Handelszeitung*. Archived from the original on 4 March 2017. Retrieved 18 September 2013.
- 161.^ Jump up to:[a](#) [b](#) unlisted (3 August 2013). "Überwachung: BND leitet massenhaft Metadaten an die NSA weiter". *Der Spiegel* (in German). Retrieved 3 August 2013.
- 162.^ 'Prolific Partner': German Intelligence Used NSA Spy Program, *Der Spiegel*. Retrieved 21 July 2013.
- 163.^ "Verfassungsschutz beliefert NSA". *Süddeutsche Zeitung* (in German). Retrieved 14 September 2013. Seit Juli 2013 testet der Verfassungsschutz die Späh- und Analysesoftware XKeyscore. Sollte der Geheimdienst das Programm im Regelbetrieb nutzen, hat sich das BfV verpflichtet, alle Erkenntnisse mit der NSA zu teilen. Das hatte der Präsident des Bundesamtes, Hans-

- Georg Maaßen, dem US-Dienst zugesichert. Im Januar und Mai war Maaßen zu Besuchen bei der NSA.
- 164.^ "Verfassungsschutz beliefert NSA". *Süddeutsche Zeitung* (in German). Retrieved 14 September 2013.
- 165.^ Glenn Greenwald, Laura Poitras & Ewen MacAskill (11 September 2013). "NSA shares raw intelligence including Americans' data with Israel". *The Guardian*. Retrieved 14 September 2013.
- 166.^ Olmer, Bart. "Ook AIVD bespiedt internetter". *De Telegraaf* (in Dutch). Retrieved 10 September 2013. Niet alleen Amerikaanse inlichtingendiensten monitoren internetters wereldwijd. Ook Nederlandse geheime diensten krijgen informatie uit het omstreden surveillanceprogramma 'Prism'.
- 167.^ Jump up to:^a ^b Dorling, Philip. "Australian spies in global deal to tap undersea cables". *The Sydney Morning Herald*. Retrieved 29 August 2013.
- 168.^ Jump up to:^a ^b "Sverige deltog i NSA-övervakning". *Svenska Dagbladet* (in Swedish). Retrieved 10 September 2013.
- 169.^ Christof Moser & Alan Cassidy. "Geheimdienst-Aufsicht will Kooperation des NDB mit der NSA prüfen" (in German). Schweiz am Sonntag. Retrieved 18 September 2013. Die NSA hat sowohl mit der Schweiz wie Dänemark eine geheime Vereinbarung abgeschlossen, die den Austausch von Geheimdienstinformationen regelt. Die Vereinbarung berechtigt die NSA, eigene Schlüsselbegriffe in die Abhörsysteme beider Staaten einspeisen zu lassen. Im Tausch für damit gewonnene Erkenntnisse der schweizerischen und dänischen Auslandsaufklärung erhalten der NDB und der dänische Geheimdienst PET von der NSA Informationen, die sie im eigenen Land aufgrund gesetzlicher Schranken nicht selber sammeln dürfen. Das geheime Abkommen macht auch die Schweiz zu einem NSA-Horchposten.
- 170.^ John Goetz, Hans Leyendecker & Frederik Obermaier (28 August 2013). "British Officials Have Far-Reaching Access To Internet And Telephone Communications". Retrieved 28 August 2013.
- 171.^ "Edward Snowden Interview: The NSA and Its Willing Helpers". *Der Spiegel*. 8 July 2013. Retrieved 29 August 2013. Snowden: Yes, of course. We're (the NSA) in bed together with the Germans the same as with most other Western countries.
- 172.^ Laura Poitras, Marcel Rosenbach & Holger Stark (12 August 2013). "Ally and Target: US Intelligence Watches Germany Closely". *Der Spiegel*. Retrieved 29 August 2013. The NSA classifies about 30 other countries as "3rd parties," with whom it cooperates, though with reservations. Germany is one of them. "We can, and often do, target the signals of most 3rd party foreign partners," the secret NSA document reads.
- 173.^ "Thatcher 'spied on ministers'". BBC. 25 February 2000.
- 174.^ Vernon Loeb (12 December 1998). "NSA Admits to Spying on Princess Diana". *The Washington Post*.
- 175.^ "Officials: NSA Scheme Foiled Terrorist Plots In Over 20 Countries". BusinessInsider. 5 August 2013. Retrieved 21 July 2015.
- 176.^ "Liberty and Security in a Changing World" (PDF). *whitehouse.gov*. Archived (PDF) from the original on 24 January 2017. Retrieved 21 July 2015 – via National Archives. since the enactment of section 702, the Committee "has not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law.

- 177.^ "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court" (PDF). Privacy and Civil Liberties Oversight Board. Archived from the original (PDF) on 23 June 2015. Retrieved 21 July 2015. In talking to dozens of career employees throughout the intelligence agencies, we found widespread dedication to the Constitution and eagerness to comply with whatever rules are laid down by Congress and the judiciary.
- 178.^ Jump up to:^a ^b Laura Poitras, Marcel Rosenbach & Holger Stark (12 August 2013). "Ally and Target: US Intelligence Watches Germany Closely". *Der Spiegel*. Retrieved 13 August 2013.
- 179.^ DeYoung, Karen (12 August 2013). "Colombia asks Kerry to explain NSA spying". *The Washington Post*. Retrieved 13 August 2013.
- 180.^ "Greenwald diz que espionagem dá vantagens comerciais e industriais aos Estados Unidos" (in Portuguese). Federal Senate of Brazil. Retrieved 13 August 2013.
- 181.^ "Greenwald diz que EUA espionam para obter vantagens comerciais" (in Portuguese). Deutsche Welle. Retrieved 13 August 2013.
- 182.^ Jump up to:^a ^b "Exclusive: U.S. directs agents to cover up program used to investigate Americans". *Reuters*. 5 August 2013. Retrieved 14 August 2013.
- 183.^ Kelley, Michael (27 August 2013). "Most NSA Abuses Are Self-Reported". Business Insider.
- 184.^ Jump up to:^a ^b United States Senate (19 November 2003). "S. Hrg. 108-491 - AGROTERRORISM: THE THREAT TO AMERICA'S BREADBASKET". U.S. Government Printing Office. Retrieved 22 September 2022.

- "The NSA Files". *The Guardian*. London. 8 June 2013. Dozens of articles about the U.S. National Security Agency and its spying and surveillance programs
- *CriMNet Evaluation Report* by the Office of the Legislative Auditor of Minnesota, March 2004; part of a program to improve sharing of criminal justice information.
- Smyth, Daniel. "Avoiding Bloodshed? US Journalists and Censorship in Wartime", *War & Society*, Volume 32, Issue 1, 2013. doi:10.1179/0729247312Z.00000000017.
- Deflem, Mathieu; Silva, Derek, M.D.; and Anna S. Rogers. 2018. "Domestic Spying: A Historical-Comparative Perspective". pp. 109–125 in *The Cambridge Handbook of Social Problems*, Volume 2, edited by A. Javier Treviño. New York: Cambridge University Press.