List of Government Mass Surveillance Projects

From Wikipedia, the free encyclopedia

*Main article:*[*Mass surveillance*](https://en.wikipedia.org/wiki/Mass_surveillance)

This is a **list of government surveillance projects** and related databases throughout the world.

* [**ECHELON**](https://en.wikipedia.org/wiki/ECHELON): A [signals intelligence](https://en.wikipedia.org/wiki/Signals_intelligence) (SIGINT) collection and analysis network operated on behalf of the five signatory states to the [UKUSA Security Agreement](https://en.wikipedia.org/wiki/UKUSA_Agreement).

**European Union**

* [**Data Retention Directive**](https://en.wikipedia.org/wiki/Data_Retention_Directive): A directive requiring EU member states to store citizens' telecommunications data for six to 24 months and allowing police and security agencies to request access from a court to details such as IP address and time of use of every email, phone call, and text message sent or received.
* [**INDECT**](https://en.wikipedia.org/wiki/INDECT): Research project funded by the [European Union](https://en.wikipedia.org/wiki/European_Union) to develop surveillance methods (e.g. processing of CCTV camera data streams) for the monitoring of abnormal behaviors in an [urban](https://en.wikipedia.org/wiki/Urban_area) environment.
* [**Schengen Information System**](https://en.wikipedia.org/wiki/Schengen_Information_System): A database kept for [national security](https://en.wikipedia.org/wiki/National_security) and [law enforcement](https://en.wikipedia.org/wiki/Law_enforcement) purposes.

National

**Australia**

*Main article:*[*Mass surveillance in Australia*](https://en.wikipedia.org/wiki/Mass_surveillance_in_Australia)

* In August 2014 it was reported that law-enforcement agencies had been accessing Australians' web browsing histories via [internet providers](https://en.wikipedia.org/wiki/Internet_provider) such as Telstra without a warrant.
* It was reported[[3]](https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects#cite_note-3) that Australia had issued 75% more wiretap warrants in 2003 than the US did and this was 26 times greater than the US on a per capita basis.

**China**

*Main article:*[*Mass surveillance in China*](https://en.wikipedia.org/wiki/Mass_surveillance_in_China)

* [**Golden Shield Project**](https://en.wikipedia.org/wiki/Golden_Shield_Project): Also known as the "Great Firewall of China", it is a [censorship](https://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China) and [surveillance](https://en.wikipedia.org/wiki/Surveillance) project operated by the [Ministry of Public Security](https://en.wikipedia.org/wiki/Ministry_of_Public_Security_of_the_People%27s_Republic_of_China) (MPS) division of the [government of the People's Republic of China](https://en.wikipedia.org/wiki/Government_of_China). The project was initiated in 1998 and began operations in November 2003.
* **Monitoring Bureau**
* **Public Information Network Security**

**France**



[DGSE](https://en.wikipedia.org/wiki/DGSE) base near [Domme](https://en.wikipedia.org/wiki/Domme,_Dordogne) in southwestern France

* [**Frenchelon**](https://en.wikipedia.org/wiki/Frenchelon): A data collection and analysis network operated by the French [Directorate-General for External Security](https://en.wikipedia.org/wiki/Directorate-General_for_External_Security).

**Germany**

* [**Nachrichtendienstliches Informationssystem**](https://en.wikipedia.org/wiki/Nachrichtendienstliches_Informationssystem): a searchable database operated by the German security agency [Bundesamt für Verfassungsschutz](https://en.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Verfassungsschutz) (BfV).
* [**Project 6**](https://en.wikipedia.org/wiki/Project_6): a [global surveillance](https://en.wikipedia.org/wiki/Global_surveillance) project jointly operated by the German intelligence agencies [Bundesnachrichtendienst](https://en.wikipedia.org/wiki/Bundesnachrichtendienst)(BND) and [Bundesamt für Verfassungsschutz](https://en.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Verfassungsschutz) (BfV) in close cooperation with the U.S. [Central Intelligence Agency](https://en.wikipedia.org/wiki/Central_Intelligence_Agency) (CIA).

**India**

*Further information:*[*Mass surveillance in India*](https://en.wikipedia.org/wiki/Mass_surveillance_in_India)

* [**Central Monitoring System**](https://en.wikipedia.org/wiki/Central_Monitoring_System) (CMS): A data collection system similar to the NSA's [PRISM](https://en.wikipedia.org/wiki/PRISM_(surveillance_program)) program. It enables the Government to listen to phone conversations, intercept [e-mails](https://en.wikipedia.org/wiki/E-mail) and text messages, monitor posts on [social networking service](https://en.wikipedia.org/wiki/Social_networking_service) and track searches on [Google](https://en.wikipedia.org/wiki/Google).
* [**DRDO NETRA**](https://en.wikipedia.org/wiki/DRDO_NETRA): Network that is capable of tracking online communications on a real time basis by harvesting data from various [voice-over-IP](https://en.wikipedia.org/wiki/Voice-over-IP) services, including Skype and [Google Talk](https://en.wikipedia.org/wiki/Google_Talk). It is operated by the [Research and Analysis Wing](https://en.wikipedia.org/wiki/Research_and_Analysis_Wing).
* [**NATGRID**](https://en.wikipedia.org/wiki/NATGRID): An intelligence grid that links the databases of several departments and ministries of the Government of India.

**Russia**

* [**SORM**](https://en.wikipedia.org/wiki/SORM): A technical system used by the [Federal Security Service of the Russian Federation](https://en.wikipedia.org/wiki/Federal_Security_Service_of_the_Russian_Federation) to monitor [internet](https://en.wikipedia.org/wiki/Internet) and [telephone](https://en.wikipedia.org/wiki/Telephone) communication.
* [**Yarovaya Law**](https://en.wikipedia.org/wiki/Yarovaya_Law) is an anti-terrorist legislation that includes requirement to store all voice and text messaging data, as well as providing cryptographic backdoors for security services.

**Sweden**

* [**Titan traffic database**](https://en.wikipedia.org/wiki/Titan_traffic_database): A [database](https://en.wikipedia.org/wiki/Database) established by the [Swedish National Defense Radio Establishment](https://en.wikipedia.org/wiki/Swedish_National_Defence_Radio_Establishment) (Swedish: Försvarets Radioanstalt, FRA) where [call detail records](https://en.wikipedia.org/wiki/Call_detail_record) (CDRs) of [telephony](https://en.wikipedia.org/wiki/Telephony) and [internet](https://en.wikipedia.org/wiki/Internet) [traffic](https://en.wikipedia.org/wiki/Traffic) and [transaction](https://en.wikipedia.org/wiki/Database_transaction) data (IPDRs) concerning international telecommunications are stored.
* [**X-Keyscore**](https://en.wikipedia.org/wiki/X-Keyscore): A system used by the United States National Security Agency for searching and analyzing internet data about foreign nationals. FRA has been granted access to the program.

**Switzerland**

* [**Onyx**](https://en.wikipedia.org/wiki/Onyx_(interception_system)): A data gathering system maintained by several [Swiss intelligence agencies](https://en.wikipedia.org/wiki/Swiss_intelligence_agencies) to monitor military and civilian communications, such as [e-mails](https://en.wikipedia.org/wiki/E-mails), [telefax](https://en.wikipedia.org/wiki/Fax) and telephone calls. In 2001, Onyx received its second nomination for the ironically-named "[Big Brother Award](https://en.wikipedia.org/wiki/Big_Brother_Awards)".

**United Kingdom**

*Further information:*[*Mass surveillance in the United Kingdom*](https://en.wikipedia.org/wiki/Mass_surveillance_in_the_United_Kingdom)

* [**Impact Nominal Index**](https://en.wikipedia.org/wiki/Impact_Nominal_Index): The Impact Nominal Index or INI is a computer system that enables the UK police force to establish whether other relevant authorities are holding information regarding a person of interest.
* [**Interception Modernization Program**](https://en.wikipedia.org/wiki/Interception_Modernisation_Programme): An initiative to extend the [UK government](https://en.wikipedia.org/wiki/UK_government)'s capability to [lawfully intercept](https://en.wikipedia.org/wiki/Lawful_interception) and store [communications data](https://en.wikipedia.org/wiki/Communications_data) in a central database.
* [**Mastering the Internet**](https://en.wikipedia.org/wiki/Mastering_the_Internet) (MTI): A clandestine [mass surveillance](https://en.wikipedia.org/wiki/Mass_surveillance) program led by the British intelligence agency [GCHQ](https://en.wikipedia.org/wiki/GCHQ). Data gathered by the GCHQ include the contents of [email](https://en.wikipedia.org/wiki/Email) messages, entries on the social networking platform [Facebook](https://en.wikipedia.org/wiki/Facebook) and the [web browsing history](https://en.wikipedia.org/wiki/Web_browsing_history) of internet users.
* [**UK National DNA Database**](https://en.wikipedia.org/wiki/United_Kingdom_National_DNA_Database) (NDNAD): It is also the oldest national DNA database in the world.[[15]](https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects#cite_note-ncbihelen-15) Since its establishment in 1995, the database has grown to include DNA samples from 2.7 million individuals, or 5.2% of the UK's population, many of whom have neither been charged with, or convicted of, any offence.
* [**Tempora**](https://en.wikipedia.org/wiki/Tempora): Launched in the autumn of 2011, this initiative allows the [GCHQ](https://en.wikipedia.org/wiki/GCHQ) to set up a large-scale [buffer](https://en.wikipedia.org/wiki/Data_buffer) that is capable of storing internet content for 3 days and metadata for 30 days.
* [**Royal Concierge**](https://en.wikipedia.org/wiki/Royal_Concierge): prototyped in 2010, sends daily alerts to [GCHQ](https://en.wikipedia.org/wiki/Government_Communications_Headquarters) whenever a booking is made from a ".gov." [second-level domain](https://en.wikipedia.org/wiki/Second-level_domain) at select hotels worldwide.

**United States**

|  |
| --- |
| [**National Security Agency**](https://en.wikipedia.org/wiki/National_Security_Agency)[**surveillance**](https://en.wikipedia.org/wiki/Terrorist_Surveillance_Program) |
| [Map of global NSA data collection](https://en.wikipedia.org/wiki/Boundless_Informant) |
| **Programs**  **Pre-1978**   * [ECHELON](https://en.wikipedia.org/wiki/ECHELON) * [MINARET](https://en.wikipedia.org/wiki/Project_MINARET) * [SHAMROCK](https://en.wikipedia.org/wiki/Project_SHAMROCK) * [PROMIS](https://en.wikipedia.org/wiki/Inslaw)   **Since 1978**   * [Upstream collection](https://en.wikipedia.org/wiki/Upstream_collection) * [BLARNEY](https://en.wikipedia.org/wiki/Blarney_(code_name)) * [FAIRVIEW](https://en.wikipedia.org/wiki/Fairview_(surveillance_program)) * [Main Core](https://en.wikipedia.org/wiki/Main_Core) * [ThinThread](https://en.wikipedia.org/wiki/ThinThread) * [Genoa](https://en.wikipedia.org/wiki/Project_Genoa)   **Since 2001**   * [OAKSTAR](https://en.wikipedia.org/wiki/OAKSTAR) * [STORMBREW](https://en.wikipedia.org/wiki/STORMBREW) * [Trailblazer](https://en.wikipedia.org/wiki/Trailblazer_Project) * [Turbulence](https://en.wikipedia.org/wiki/Turbulence_(NSA)) * [Genoa II](https://en.wikipedia.org/wiki/Project_Genoa_II) * [Total Information Awareness](https://en.wikipedia.org/wiki/Total_Information_Awareness) * [President's Surveillance Program](https://en.wikipedia.org/wiki/President%27s_Surveillance_Program)   + [Terrorist Surveillance Program](https://en.wikipedia.org/wiki/Terrorist_Surveillance_Program)   **Since 2007**   * [PRISM](https://en.wikipedia.org/wiki/PRISM_(surveillance_program)) * [Dropmire](https://en.wikipedia.org/wiki/Dropmire) * [Stateroom](https://en.wikipedia.org/wiki/Stateroom_(surveillance_program)) * [Bullrun](https://en.wikipedia.org/wiki/Bullrun_(code_name)) * [MYSTIC](https://en.wikipedia.org/wiki/MYSTIC_(surveillance_program)) * [MonsterMind](https://en.wikipedia.org/wiki/MonsterMind) (alleged)   **Databases, tools etc.**   * [PINWALE](https://en.wikipedia.org/wiki/PINWALE) * [MARINA](https://en.wikipedia.org/wiki/MARINA) * [MAINWAY](https://en.wikipedia.org/wiki/MAINWAY) * [TRAFFICTHIEF](https://en.wikipedia.org/wiki/TRAFFICTHIEF) * [DISHFIRE](https://en.wikipedia.org/wiki/Dishfire) * [XKeyscore](https://en.wikipedia.org/wiki/XKeyscore) * [ICREACH](https://en.wikipedia.org/wiki/ICREACH) * [BOUNDLESSINFORMANT](https://en.wikipedia.org/wiki/Boundless_Informant)   **GCHQ collaboration**   * [MUSCULAR](https://en.wikipedia.org/wiki/MUSCULAR_(surveillance_program)) * [Tempora](https://en.wikipedia.org/wiki/Tempora) |
| **Legislation** |
| **Institutions** |
| **Lawsuits** |
| **Whistleblowers** |
| **Publication** |
| **Related** |
| **Concepts** |
| **Collaboration** |

*Further information:*[*Mass surveillance in the United States*](https://en.wikipedia.org/wiki/Mass_surveillance_in_the_United_States)

A [top secret](https://en.wikipedia.org/wiki/Top_secret) document leaked by [Edward Snowden](https://en.wikipedia.org/wiki/Edward_Snowden) to [*The Guardian*](https://en.wikipedia.org/wiki/The_Guardian) in 2013, originally due to be declassified on 12 April 2038.

* [**Boundless Informant**](https://en.wikipedia.org/wiki/Boundless_Informant): A system deployed by the [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) to analyze global electronic information. In March 2013, Boundless Informant gathered 14 billion data reports from [Iran](https://en.wikipedia.org/wiki/Iran), 6.3 billion from [India](https://en.wikipedia.org/wiki/India), and 2.8 billion from the [United States](https://en.wikipedia.org/wiki/United_States).
* [**BULLRUN**](https://en.wikipedia.org/wiki/Bullrun_(code_name)): a highly classified U.S. [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) program to preserve its ability to eavesdrop on encrypted communications by influencing and weakening encryption standards, by obtaining master encryption keys, and by gaining access to data before or after it is encrypted either by agreement, by force of law, or by computer network exploitation (hacking).
* [**Carnivore**](https://en.wikipedia.org/wiki/Carnivore_(software)): A system implemented by the Federal Bureau of Investigation that was designed to monitor email and electronic communications. Apparently replaced by commercial software such as [NarusInsight](https://en.wikipedia.org/wiki/NarusInsight).
* [**Comprehensive National Cybersecurity Initiative**](https://en.wikipedia.org/wiki/Comprehensive_National_Cybersecurity_Initiative)
* [**DCSNet**](https://en.wikipedia.org/wiki/DCSNet): The [Federal Bureau of Investigation](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) (FBI)'s [point-and-click](https://en.wikipedia.org/wiki/Point-and-click) surveillance system that can perform instant wiretaps on any telecommunications device located in the [United States](https://en.wikipedia.org/wiki/United_States).
* [**Fairview**](https://en.wikipedia.org/wiki/Fairview_(surveillance_program)): A [mass surveillance](https://en.wikipedia.org/wiki/Mass_surveillance) program directed at foreign mobile phone users.
* [**Financial Crimes Enforcement Network**](https://en.wikipedia.org/wiki/Financial_Crimes_Enforcement_Network): A bureau of the [Department of the Treasury](https://en.wikipedia.org/wiki/United_States_Department_of_the_Treasury) that collects and analyzes financial transactions in order to combat [financial crimes](https://en.wikipedia.org/wiki/Financial_crimes).
* [**ICREACH**](https://en.wikipedia.org/wiki/ICREACH): Surveillance [frontend](https://en.wikipedia.org/wiki/Front_and_back_ends) [GUI](https://en.wikipedia.org/wiki/Graphical_user_interface) that is shared with 23 government agencies, including the [CIA](https://en.wikipedia.org/wiki/Central_Intelligence_Agency), [DEA](https://en.wikipedia.org/wiki/Drug_Enforcement_Administration), and [FBI](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation), to search illegally collected personal records.
* [**Magic Lantern**](https://en.wikipedia.org/wiki/Magic_Lantern_(software)): A [keystroke logging](https://en.wikipedia.org/wiki/Keystroke_logging) [software](https://en.wikipedia.org/wiki/Software) deployed by the FBI in the form of an [e-mail attachment](https://en.wikipedia.org/wiki/E-mail_attachment). When activated, it acts as a [trojan horse](https://en.wikipedia.org/wiki/Trojan_horse) and allows the FBI to decrypt user communications.
* [**Main Core**](https://en.wikipedia.org/wiki/Main_Core): A personal and financial database storing information of millions of U.S. citizens believed to be threats to [national security](https://en.wikipedia.org/wiki/National_security). The data mostly comes from the [NSA](https://en.wikipedia.org/wiki/National_Security_Agency), [FBI](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation), [CIA](https://en.wikipedia.org/wiki/Central_Intelligence_Agency), as well as other government sources.
* [**MAINWAY**](https://en.wikipedia.org/wiki/MAINWAY): NSA database containing [metadata](https://en.wikipedia.org/wiki/Metadata) for hundreds of billions of [telephone calls](https://en.wikipedia.org/wiki/Telephone_call) made through the four largest [telephone carriers](https://en.wikipedia.org/wiki/Telephone_company) in the United States.
* [**Media monitoring services**](https://en.wikipedia.org/wiki/DHS_media_monitoring_services), A proposed DHS database for monitoring all global news sources and media influencers.
* [**MUSCULAR**](https://en.wikipedia.org/wiki/Muscular_(surveillance_program)): Overseas wiretapping of [Google](https://en.wikipedia.org/wiki/Google#Google_data_centers)'s and [Yahoo](https://en.wikipedia.org/wiki/Yahoo#Privacy)'s unencrypted internal networks by the NSA.
* [**MYSTIC**](https://en.wikipedia.org/wiki/MYSTIC_(surveillance_program)) is a voice interception program used by the National Security Agency.
* [**Nationwide Suspicious Activity Reporting Initiative**](https://en.wikipedia.org/wiki/Nationwide_Suspicious_Activity_Reporting_Initiative): Under this government initiative, a [Suspicious Activity Report](https://en.wikipedia.org/wiki/Suspicious_Activity_Report_(justice_and_homeland_security)) (SAR) may be filed by law enforcers, public safety personnel, owners of critical infrastructure or the general public.
* [**NSA ANT catalog**](https://en.wikipedia.org/wiki/NSA_ANT_catalog)**:** a 50-page document listing technology available to the United States National Security Agency (NSA) ANT division to aid in cyber-surveillance.
* [**PRISM**](https://en.wikipedia.org/wiki/PRISM_(surveillance_program)): A clandestine national security electronic surveillance program operated by the United States National Security Agency (NSA) which can target customers of participating corporations outside or inside the United States.
* [**Room 641A**](https://en.wikipedia.org/wiki/Room_641A): A telecommunication interception facility operated by [AT&T](https://en.wikipedia.org/wiki/AT%26T) for the U.S. National Security Agency.
* [**Sentry Eagle**](https://en.wikipedia.org/wiki/Sentry_Eagle): efforts to monitor and attack an adversary's cyberspace through capabilities include SIGINT, Computer Network Exploitation (CNE), Information Assurance, Computer Network Defense (CND), Network Warfare, and Computer Network Attack (CNA). The efforts included weakening US commercial encryption systems.
* [**Special Collection Service**](https://en.wikipedia.org/wiki/Special_Collection_Service) (SCS): A [black budget](https://en.wikipedia.org/wiki/Black_budget) program that is responsible for "close surveillance, burglary, wiretapping, breaking and entering." It employs [covert listening device](https://en.wikipedia.org/wiki/Covert_listening_device) technologies to bug foreign embassies, communications centers, computer facilities, fiber-optic networks, and government installations.
* [**Stellar Wind (code name)**](https://en.wikipedia.org/wiki/Stellar_Wind): The [open secret](https://en.wikipedia.org/wiki/Open_secret) [code name](https://en.wikipedia.org/wiki/Code_name) for four surveillance programs.
* [**Tailored Access Operations**](https://en.wikipedia.org/wiki/Tailored_Access_Operations): Intelligence-gathering unit of the NSA that is capable of harvesting approximately 2[petabytes](https://en.wikipedia.org/wiki/Petabyte) of data per hour.
* [**Terrorist Finance Tracking Program**](https://en.wikipedia.org/wiki/Terrorist_Finance_Tracking_Program): A joint initiative run by the [CIA](https://en.wikipedia.org/wiki/Central_Intelligence_Agency) and the [Department of the Treasury](https://en.wikipedia.org/wiki/United_States_Department_of_the_Treasury) to access the SWIFT ([Society for Worldwide Interbank Financial Telecommunication](https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication)) transaction database as part of the [Bush administration](https://en.wikipedia.org/wiki/George_W._Bush_administration)'s "Global [War on Terrorism](https://en.wikipedia.org/wiki/War_on_Terrorism)". According to the U.S. government, its efforts to [counter terrorist activities](https://en.wikipedia.org/wiki/Counter-terrorism) were compromised after the existence of the Terrorist Finance Tracking Program was leaked to the media.
* [**Turbulence**](https://en.wikipedia.org/wiki/Turbulence) (NSA): Turbulence is a United States National Security Agency (NSA) information-technology project started circa 2005. It was developed in small, inexpensive "test" pieces rather than one grand plan like its failed predecessor, the Trailblazer Project. It also includes offensive cyberwarfare capabilities, like injecting malware into remote computers. The U.S. Congress criticized the project in 2007 for having similar bureaucratic problems as the Trailblazer Project.
* [**US Intelligence Community**](https://en.wikipedia.org/wiki/United_States_Intelligence_Community) (IC): A cooperative federation of 16 government agencies working together, but also separately, to gather intelligence and conduct espionage.
* [**Utah Data Center**](https://en.wikipedia.org/wiki/Utah_Data_Center): The Intelligence Community's US$1.5 billion [data storage](https://en.wikipedia.org/wiki/Computer_data_storage) center that is designed to store extremely large amounts of data, on the scale of yottabytes.
* [**X-Keyscore**](https://en.wikipedia.org/wiki/X-Keyscore): A system used by the United States National Security Agency for searching and analyzing internet data about foreign nationals.

Unclear origin

* [**GhostNet**](https://en.wikipedia.org/wiki/GhostNet): A fictitious code name given to a large-scale surveillance project that is believed to be operated by the [People's Republic of China](https://en.wikipedia.org/wiki/People%27s_Republic_of_China).
* [**Stuxnet**](https://en.wikipedia.org/wiki/Stuxnet): It is the first discovered [malware](https://en.wikipedia.org/wiki/Malware) that spies on industrial systems, and it was used to attack [Iran](https://en.wikipedia.org/wiki/Iran)'s nuclear facilities. It is believed to have originated from the [United States](https://en.wikipedia.org/wiki/United_States) under the [Bush administration](https://en.wikipedia.org/wiki/Presidency_of_George_W._Bush).

Recently discontinued

* [*Information Awareness Office*](https://en.wikipedia.org/wiki/Information_Awareness_Office): An office established to bring together several DARPA projects focused on applying surveillance and information technology to track and monitor terrorists and other threats to U.S. national security.
* [**Multistate Anti-Terrorism Information Exchange**](https://en.wikipedia.org/wiki/Multistate_Anti-Terrorism_Information_Exchange) (MATRIX): A [data mining system](https://en.wikipedia.org/wiki/Data_mining_system) originally developed for the [Florida Department of Law Enforcement](https://en.wikipedia.org/wiki/Florida_Department_of_Law_Enforcement).
* [**Terrorist Surveillance Program**](https://en.wikipedia.org/wiki/Terrorist_Surveillance_Program): Replaced by [PRISM](https://en.wikipedia.org/wiki/PRISM_(surveillance_program)).
* [**ThinThread**](https://en.wikipedia.org/wiki/ThinThread): A U.S. National Security Agency (NSA) program that involved wiretapping and sophisticated analysis of the resulting data.
* [**Trailblazer Project**](https://en.wikipedia.org/wiki/Trailblazer_Project): U.S. National Security Agency (NSA) program intended to develop a capability to analyze data carried on communications networks including cell phone networks and the Internet.