There are 3,984 federal, state and local organizations working on domestic counterterrorism. Most collect information on people in the US. [1]

92 million documents are classified in a year and more than 4 million Americans have security clearance [2]

In 2012 the government made 1,856 applications for electronic surveillance to **FISA**. **None was denied.** Telecoms that had agreed to participate in the activity were granted immunity from prosecution and lawsuits. [2]

Number of communications intercepted since 9/11: "between 15 and 20 trillion" 3

NSA stores Americans' **phone records, emails and text messages**, uses corporate proxies to monitor up to 75 percent of internet traffic in the US. It acquires companies' raw data—e-mails, video chats, and social media messages, which analysts then mine. [6]

NSA's Special Source Operations Branch sweeps up hundreds of millions of **contact lists from e-mail** and instant messaging accounts around the world each year. [47]

NSA has an immense data center which can intercept analyze and store electronic communications from satellites and cables across the nation and the world. [3]

NSA's Utah **data center** is a million square feet, cost $2 billion, store five trillion gigabytes, intercept 20 terabytes per minute. [5]

NSA circumvented or cracked encryption that guards global commerce, banking systems, trade secrets, medical records, and which secures e-mails, Web searches, internet chats and phone calls of Americans and others around the world. [7]

NSA collaborates with the **CIA** in targeted killing (**drone**) program.[46]

FBI's **National Security Branch Analysis Center** (NSAC) hunts terrorists, hackers and criminals and contains tens of thousands of **records from corporate databases, car-rental companies and hotel chains** on citizens and foreigners. FBI wants the database of the Airlines Reporting Corporation—billions of Americans' itineraries and methods of payment. [8]

FBI NASC has more than **1.5 billion government and private-sector records** about US citizens collected from commercial databases. [8]

The **FBI** operates the **Nationwide Suspicious Activity Reporting Initiative (SAR)**. It collects and analyzes reports of suspicious activities by local law enforcement, 160,000+ suspicious activity files. SAR stores the profiles of residents not accused of any crime. [9]

National security agencies can **share U.S. civilian information** with federal, state, local, or foreign entities for analysis even if there is no reason for suspicion. [10]

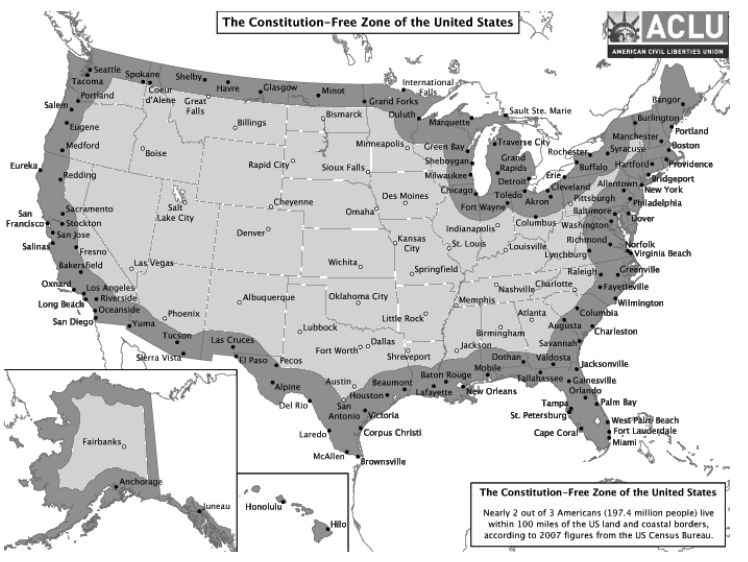
Large companies provide data to the NSA and other government agencies in return for **favored treatment**. [11]

NSA shares intelligence with **Wall Street** banks in the name of "battling hackers." [12]

Some NSA programs active in 2013

VALIDATOR
MAINWAY
UNITEDRAKE
PRISM
XKEYSCORE
TEMPORA
DRTBOX
WHITEBOX
AMHS
NUCLEON
TRAFFICTHIEF
ARCMAP
SIGNAV
COASTLINE
DISHFIRE
FASTSCOPE
OCTAVE
CONTRAOCTAVE
PINWALE
WEBCANDID
MICHIGAN
PLUS
MAINWAY
FASCIA
OCTSKYWARD
NTELINK
BANYAN
PINWALE
TURBULENCE [50]

NSA has **spied** on Germany, England, Brazil, Mexico, European Union offices in Brussels and Washington and other countries. In one month it swept up 70 million telephone calls and instant messages in France, 60 million in Spain [48]



FBI shared NSAC data with the Pentagon's Counter-Intelligence Field Activity office, a domestic-spying unit which collected data on peace groups, including the Quakers, until it was shut down in 2008. [10]

The **USPS Mail Isolation Control and Tracking** program photographs the exterior of every piece of paper mail that is processed in the US — about 160 billion pieces last year. Access by federal agents requires no warrant, just a written request. [13]

*The **US border** is an exception to the 4th Amendment of the U.S. Constitution. Authorities **do not need a warrant or probable cause** to conduct a "routine search."* [14]

*According to the government, **"the border" is a 100-mile wide strip** that wraps around the "external boundary" of the United States.* [14]

In 2008 courts upheld such constitution free zones. [15]

2/3 of the entire US population (197.4 million people) live within 100 miles of the US land and coastal borders. [14]

WSJ: the **NSA spies on Americans' credit card transactions.** [17] FBI already has full access to the database. [18] IRS computers can scan multiple networks to collect profiles for every taxpayer, including **shopping records, travel, social interactions, health records and files** from other government investigators. [19]

The **Terrorist Identities Datamart Environment (TIDE)** of the National Counterterrorism Center has **740,000+ names** of suspected terrorists, travel records of citizens and foreigners, financial forms filed by banks and casinos, 200 million records from private data brokers such Accurint, Acxiom* and Choicepoint, telephone records and wiretapped conversations captured by the FBI. [8]

***DHS** says the **search zones encompass the entire states** of Connecticut, Delaware, Florida, Hawaii, Maine, Massachusetts, Michigan, New Hampshire, New Jersey or Rhode Island.* [14]

***Customs and Border Patrol** (CBP) has been setting up **checkpoints** inland — on highways in California, Texas and Arizona, and at ferry terminals in Washington State.*[14]

"Your constitutional rights have been repealed in ten states." [16]

Government is insisting that **"black boxes"** be installed in cars to track location. [23]

The FBI admits it has about 3,000 **GPS tracking devices** on cars of unsuspecting people in the US. [24]

DEA's automated license plate readers (ALPRs) can track automobile movements. There are plans to mine the plates. DEA wants to use this "for 'intelligence" and to "research the movements" of suspects.' [25]

Virtual reality glasses can summarize in graphic form **car owners' police records,** points on his/her license, how far from home the vehicle is, owners' TSA Pre-Check score, and other data. [25]

Telecoms must employ technicians with security clearances who assist in government surveillance, but are not allowed to disclose their activities to their uncleared bosses. [5]

NSA gained warrantless access to **AT&T's and Verizon's billing records**. As of 2007, AT&T had more than 2.8 trillion records in a database. [3]

NSA has monitoring rooms in major US telecoms at junction points, gaining access to international and domestic communications. [3]

NSA monitors AT&T's earth stations and **satellite receivers**. [3]

Cell phone carriers responded to at least 1.3 million law enforcement requests for **cell phone tracking** and other data in 2011. [21]

Cell phones in the US are **tracked without warrants** by law enforcement. Tracking software can pinpoint and document phone location. Cell carriers can "clone" a phone and **download text messages while it is turned off.** [22]

Verizon filed a patent that allows a **television to track** what you are doing, who you are with, what objects you're holding, and your mood. Technology would allow cable companies to monitor habits and reactions to product advertisements. [27]

Some cell carriers **market** a catalog of "**surveillance fees**" to police departments to determine a suspect's location, trace phone calls and texts or provide other services. [22]

Police cruisers can **photograph** every **car** they pass, up to 3000 per hour. The files are stored indefinitely. [20]

The technology includes **cameras and microphones in DVRs or cable boxes**, and analyzes viewers' responses, behaviors and statements, can monitor sleeping, eating, exercising, reading and more. [28]

The **Kinect** can determine when users are viewing ads broadcast by the **Xbox** through its eye movement tracking. [29]

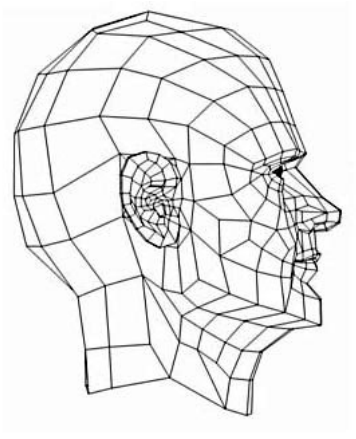
High-tech trash cans tracked people in London's financial district, measured the Wi-Fi signals emitted by smartphones, and used tracking files that follow Internet users across the Web to the physical world. London ended the program. [30]

Police in AZ have acquired their own **tracking equipment** to avoid the time and expense of having the **phone companies** do it for them. [49]

DEA's Hemisphere Project can access an **AT&T database** with decades of Americans' phone calls. DEA pays AT&T to place employees in drug-fighting units, sit with DEA agents and local detectives and supply phone data from as far back as 1987.[4]

"Just about the only place that's somewhat immune to the NSA's new style of code-breaking attacks? North Korea, because it's so disconnected from the rest of the world's networks." [50]

San Francisco, Baltimore and other cities, with funding from the **DHS**, are installing systems on buses that give the ability to **record and store private conversations**. The systems pair conversations with camera images and can couple with facial recognition systems. They can be accessed remotely and be combined with GPS data to track passengers throughout the city. [26]



New surveillance tools "can **secretly activate laptop webcams or microphones** on mobile devices," change the contents of emails nid-transmission and use voice recognition to scan phone networks. [31]

FBI wants a **backdoor** to all software. European computer publication *Heise* said in 1999 that the NSA had built a backdoor into all Windows software. [32]

"**Items of interest** will be located, identified, monitored, and remotely controlled through ... **radio-frequency identification,** sensor networks, embedded servers, and energy harvesters — connected to the internet using high-power computing." David Petraeus [34]

Smart street lights are being installed in Detroit, Chicago, Pittsburgh and elsewhere. Each has a microprocessor for wireless communication, can capture images and count people through a digital camera, record conversations and give voice commands via a built-in speaker. [38]

Customs and Border Protection offers **drones** to law-enforcement agencies and has considered equipping them with "nonlethal weapons." The CBP said data collected could be shared with other government agencies. It has lent drones to the FBI, Texas Dept. of Public Safety, and others. [36]

13 police agencies have used **drones** says the Association for Unmanned Vehicle Systems International. The FAA predicts that by the end of the decade 30,000 commercial and government drones could be flying over U.S. skies. [35] FBI told Congress that drones are used for **domestic surveillance** … and that there are no rules in place governing spying on Americans with drones. [37]

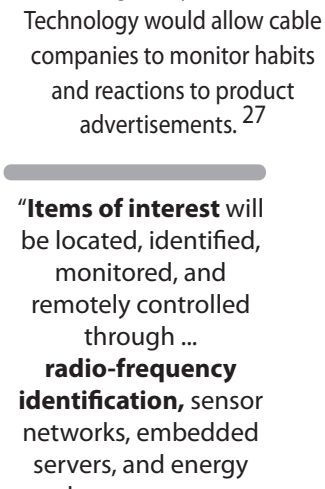
The Obama administration has plans to give all US spy agencies **full access to a massive database** that contains **financial data** on American citizens and others who bank in the country, according to a Treasury Department document. [18]

Financial institutions in the US are required by law to file reports of **"suspicious customer activity,"** such as large money transfers or unusually structured bank accounts, to Treasury's **Financial Crimes Enforcement Network (FinCEN)**. [18]

In 2013 **IRS** can track all **credit card transactions**. Agents use social media and e-commerce sites including eBay, data sent by mobile devices. The ACLU showed documents in which the IRS said the agency could look at emails without warrants. [19]

IBM **digital billboards** will read the information contained in **RFID** chips, such as a person's name, age, gender, address, and purchasing history, and then deliver a personalized ad as that person walks past. RFIDs are currently in "contact free" credit cards, and in cell phones that allow access to bank accounts and make online purchases. [39]

126+ million people have their fingerprints, photographs and biographical information accessible on the US Department of Homeland Security **Automated Biometric Identification System (IDENT)**. The system conducts about 250,000 biometric transactions each day. [40]



DNA profiles on more than ten million people are available in the FBI coordinated **Combined DNA Index System (CODIS)**.[41]

The DoD has an automated **biometric identification system** (ABIS). The database incorporates fingerprint, palm print, face and iris matching on six million people and is adding 20,000 more people each day. [42]

The **DHS** is developing a crowd-scanning project called the **Biometric Optical Surveillance System (BOSS)**. It pairs computers with video cameras to scan crowds and identify people by their faces. [45]

Police will soon have handheld devices to collect fingerprint, face, iris and **DNA information** on the spot and have it instantly sent to national databases for comparison and storage. [42]

The Maricopa AZ County sheriff's office records 9,000 **biometric** mug shots a month. [43]

"That [NSA spying] 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."
Senator Frank Church, 1975 [44]

Once the government can **spy on US citizens**, there are great temptations to abuse that power for political purposes, as when Richard Nixon eavesdropped on his political enemies during Watergate and ordered the NSA to spy on antiwar protesters. [3]

ephemera 11 /

surveillance

sources/notes on reverse

loren madsen 2013

"We are, like, that far from a turnkey totalitarian state."
Former senior NSA technical director William Binney [3]