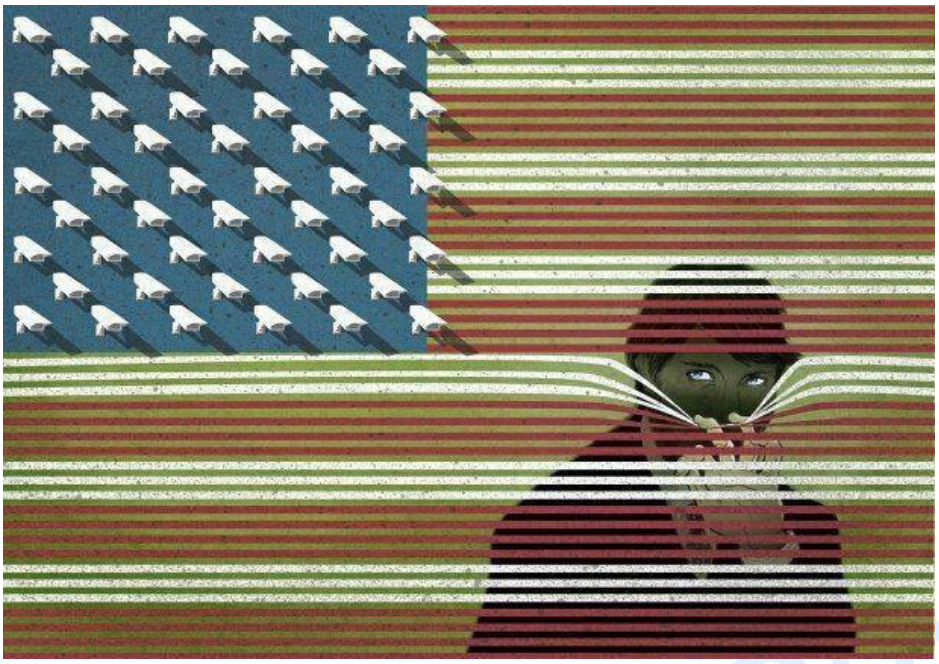
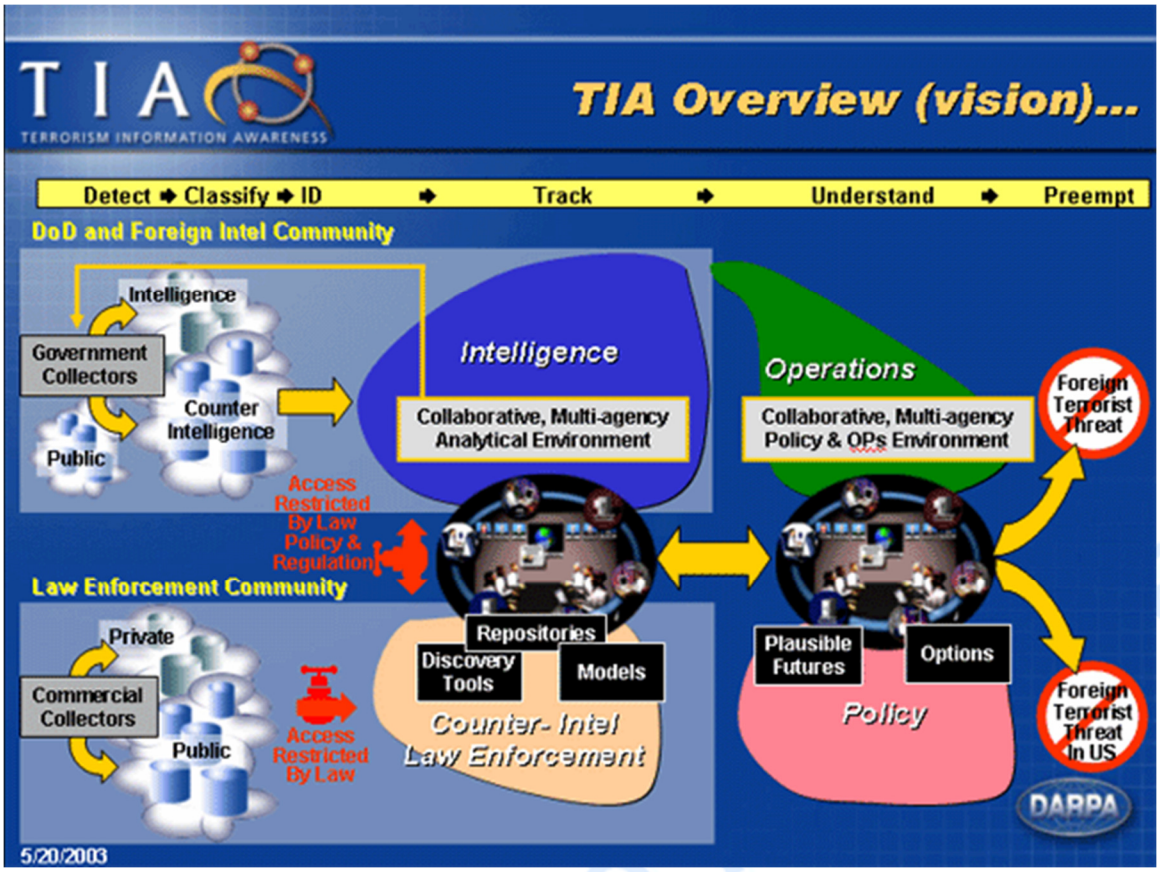
Total Surveillance In America?



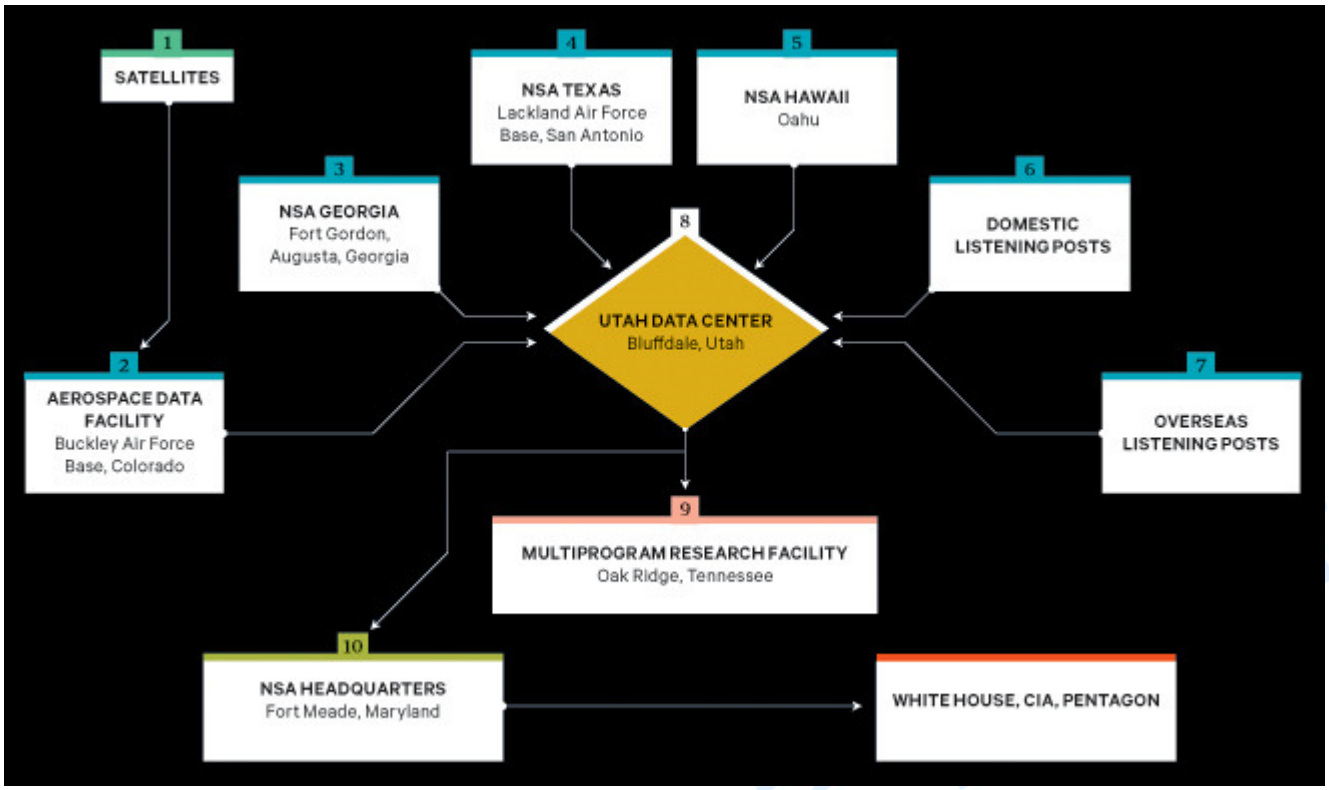
Total (Terrorist) Information Awareness is housed at the Defense Department's Advanced Research Projects Agency (DARPA). The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technologies for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface.

DARPA began as the Advanced Research Projects Agency (ARPA) created in 1958 by president Dwight D. Eisenhower for the purpose of forming and executing research and development projects to expand the frontiers of technology and science and able to reach far beyond immediate military requirements. The administration was responding to the Soviet launching of Sputnik 1 in 1957, and ARPA's mission was to ensure U.S. military technology be more sophisticated than that of the nation's potential enemies. From DARPA's own introduction.

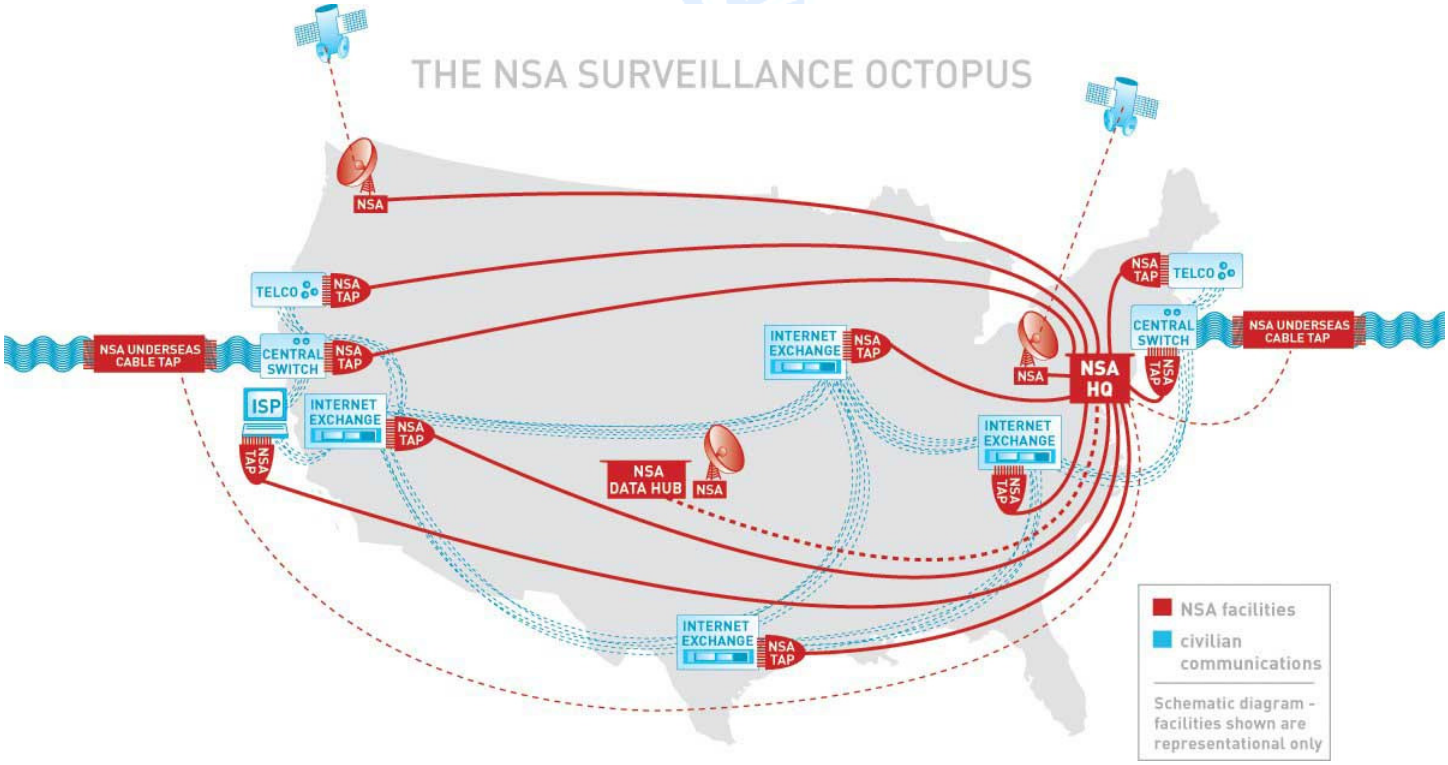


As stated, DARPA's original mission, established in 1958, was to prevent technological surprise like the launch of Sputnik, which signaled that the Soviets had beaten the U.S. into space. The mission statement has evolved over time. Today, DARPA's mission is still to prevent technological surprise to the US, but also to create technological surprise for our enemies.

From 1958 to 1965, ARPA's emphasis centered on major national issues, including space, ballistic missile defense, and nuclear test detection. During 1960, all of its civilian space programs were transferred to the National Aeronautics and Space Administration (NASA) and the military space programs to the individual Services.



ARPA, was renamed to "DARPA" (for Defense) in March 1972, then renamed "ARPA" again in February 1993, and then renamed "DARPA" again in March 1996.

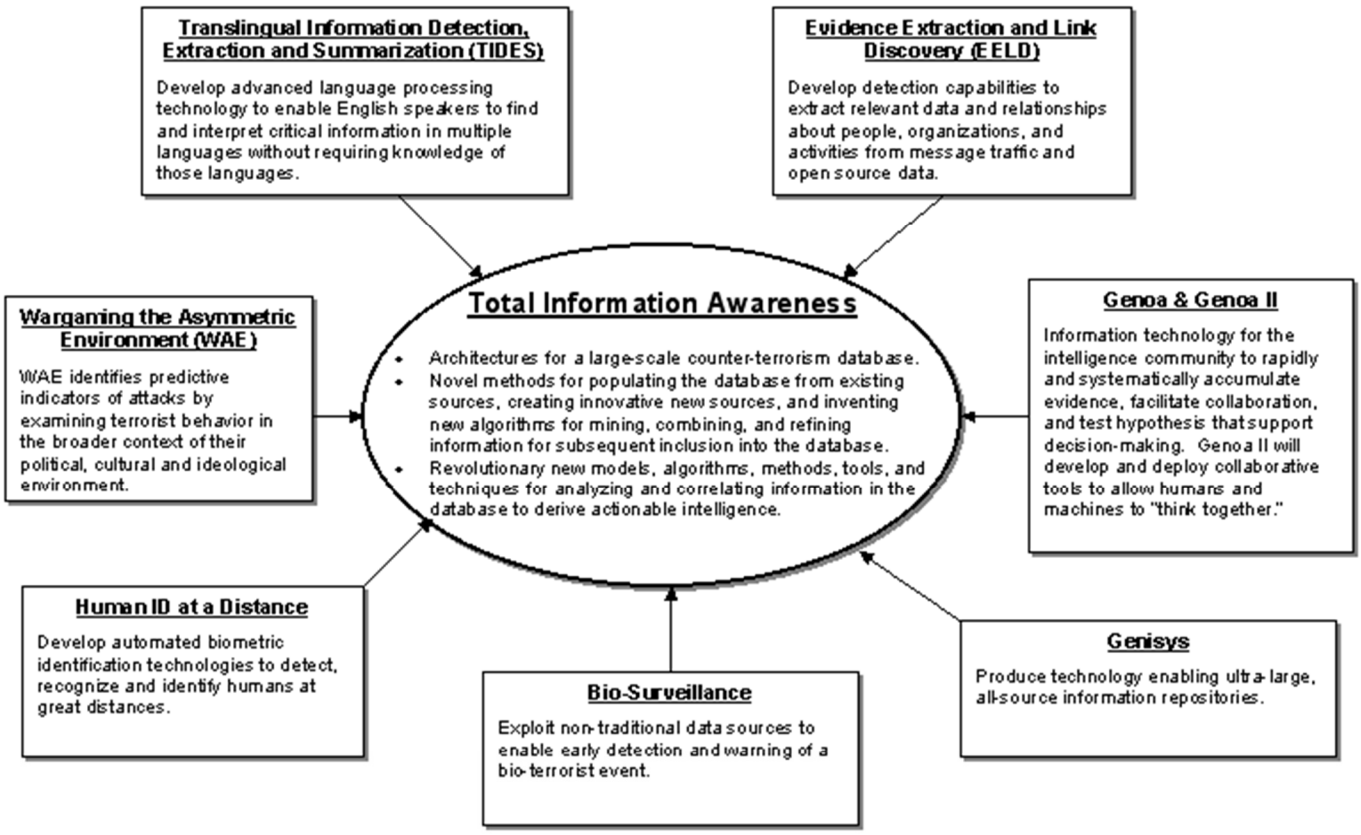


DARPA is independent from other more conventional military research and development and reports directly to senior Department of Defense management. DARPA has around 240 personnel (about 140

technical) directly managing a $3.2 billion budget. These figures are "*on average*" since DARPA focuses on short-term (two to four-year) projects run by small, purpose-built teams.

The government legislation that brought DARPA into existence are:

- Supplemental Military Construction Authorization (Air Force) (Public Law 85-325) and Department of Defense Directive 5105.15, in February 1958.
- The Mansfield Amendment of 1973 expressly limited appropriations for defense research (through ARPA/DARPA) to projects with direct military application.



"The primary goal of TIA is the assured transition of a system-level prototype that integrates technology and components developed in other DARPA programs including Genoa, Genoa-II, TIDES, Genisys, EELD, WAE, HID, and Bio-Surveillance." DARPA FY03 Budget, page 273: http://www.darpa.mil/body/pdf/FY03BudEst.pdf.

Chart text source: http://www.darpa.mil/iao/programs.htm

DARPA had many offices including IAO (Information Awareness Office). The following offices no longer "officially" exist:

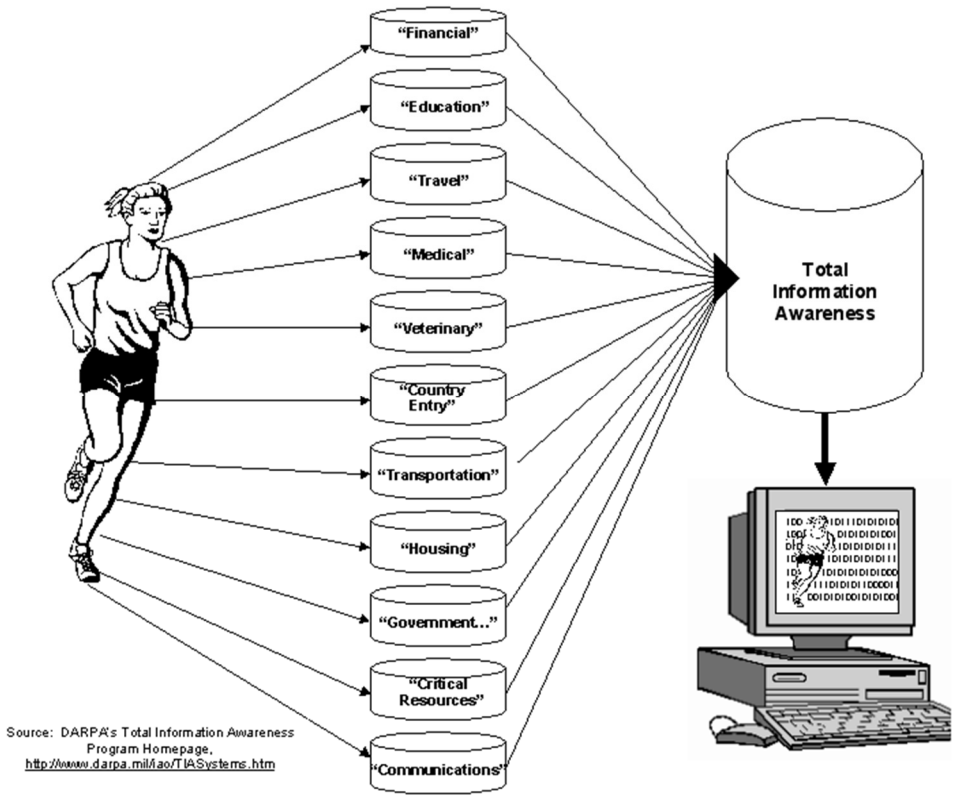
- *Information Awareness Office* - 2002–2003
- The *Advanced Technology Office (ATO)* researched, demonstrated, and developed high payoff projects in maritime, communications, special operations, command and control, and information assurance and survivability mission areas.[citation needed]
- The *Special Projects Office (SPO)* researched, developed, demonstrated, and transitioned technologies focused on addressing present and emerging national challenges. SPO investments ranged from the development of enabling technologies to the demonstration of large prototype systems. SPO developed technologies to counter the emerging threat of underground facilities used for purposes ranging from command-and-control, to weapons storage and staging, to the manufacture of weapons of mass destruction. SPO developed significantly more cost-effective ways to counter proliferated, inexpensive cruise missiles, UAVs, and other platforms used for weapon delivery, jamming, and surveillance. SPO invested in novel space technologies across the spectrum of space control applications including rapid access, space situational awareness, counterspace, and persistent tactical grade sensing approaches including extremely large space apertures and structures.
- *The Information Systems Office (ISO)* in the 1990s developed system applications of advanced information technologies. It was a predecessor to the Information Exploitation Office.

A 1991 reorganization created several offices which existed throughout the early 1990s:

- *The Electronic Systems Technology Office* combined areas of the Defense Sciences Office and the Defense Manufacturing Office. This new office will focus on the boundary between general-purpose computers and the physical world, such as sensors, displays and the first few layers of specialized signal-processing that couple these modules to standard computer interfaces.
- The *Computing Systems Technology Office* combined functions of the old Information Sciences and Tactical Technology office. The office "will work scalable parallel and distributed heterogeneous computing systems technologies," DoD said.[citation needed]
- The *Software and Intelligent Systems Technology Office and the Computing Systems office will have responsibility associated with the Presidential High-Performance Computing Initiative*. The Software office will also be responsible for "software systems technology, machine intelligence and software engineering."
- The *Land Systems Office* was created to develop advanced land vehicle and anti-armor systems, once the domain of the Tactical Technology Office
- The *Undersea Warfare Office* combined areas of the Advanced Vehicle Systems and Tactical Technology offices to develop and demonstrate submarine stealth and counterstealth and automation.

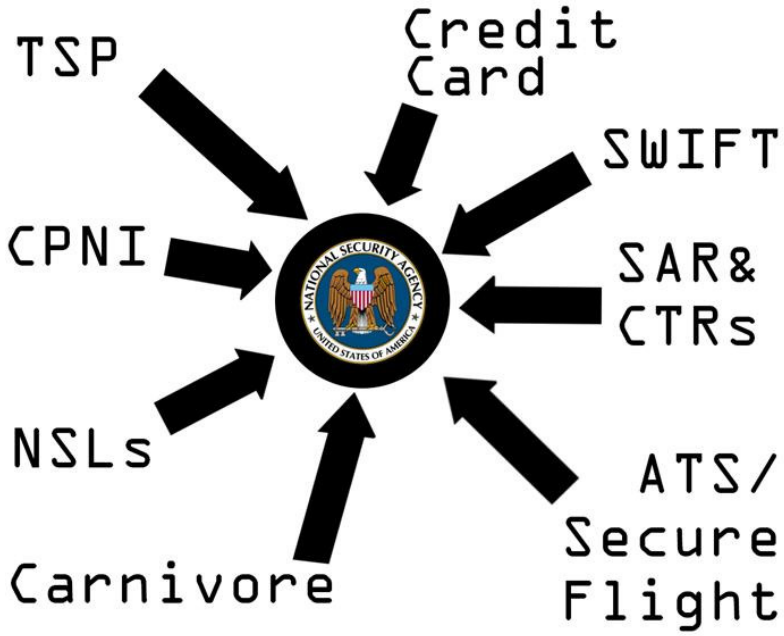
Reorganization in 2010 merged two offices; The IPTO was combined with TCTO in 2010 to form the I2O.

- The *Transformational Convergence Technology Office (TCTO)* mission was to advance new crosscutting capabilities derived from a broad range of emerging technological and social trends, particularly in areas related to computing and computing-reliant subareas of the life sciences, social sciences, manufacturing, and commerce. The TCTO was folded into the I2O in 2010.
- The *Information Processing Techniques Office (IPTO*) focused on inventing the networking, computing, and software technologies vital to ensuring DOD military superiority.



Past DARPA projects include:

Project AGILE
ARPANET, earliest predecessor of the Internet
Aspen Movie Map
ASTOVL, precursor of the Joint Strike Fighter Program[27]
Boeing X-45
CPOF - the command post of the future - networked information system for Command control.
DAML
DARPA Grand Challenge - driverless car competition
DARPA Network Challenge[28]
DEFENDER
High Performance Knowledge Bases
HISSS
Hypersonic Research Program
I3 (Intelligent Integration of Information),[29] supported the Digital Library research effort through NSF
Project MAC
Luke Arm, a DEKA creation
MOSIS
MQ-1 Predator
Multics
NLS/Augment, the origin of the canonical contemporary computer user interface
Northrop Grumman Switchblade - an unmanned oblique-wing flying aircraft for high speed, long range and long endurance flight
Onion routing
Passive radar
Policy Analysis Market
POSSE
Rapid Knowledge Formation
Sea Shadow
DARPA Shredder Challenge 2011[30] - Reconstruction of shredded documents
Strategic Computing Program
Synthetic Aperture Ladar for Tactical Applications (SALTI)
SURAN (1983–87)
Project Vela (1963)



DARPA currently has six (official) program offices, all of which report to the DARPA director:

The *Adaptive Execution Office (AEO)* is one of two new DARPA offices created in 2009 by the previous DARPA Director, Regina Dugan. Its four thrust areas include technology transition, assessment, rapid productivity and adaptive systems.

The *Defense Sciences Office (DSO)* vigorously pursues the most promising technologies within a broad spectrum of the science and engineering research communities and develops those technologies into important, radically new military capabilities.

The *Information Innovation Office (I2O)* aims to ensure U.S. technological superiority in all areas where information can provide a decisive military advantage.

The *Microsystems Technology Office (MTO)* mission focuses on the heterogeneous microchip-scale integration of electronics, photonics, and microelectromechanical systems (MEMS). Their high risk/high payoff technology is aimed at solving the national level problems of protection from biological, chemical and information attack and to provide operational dominance for mobile distributed command and control, combined manned/unmanned warfare, and dynamic, adaptive military planning and execution.

The *Strategic Technology Office (STO)* mission is to focus on technologies that have a global theater-wide impact and that involve multiple Services.[12]

The *Tactical Technology Office (TTO)* engages in high-risk, high-payoff advanced military research, emphasizing the "system" and "subsystem" approach to the development of aeronautic, space, and land systems as well as embedded processors and control systems. This research includes an effort within the TTO to develop a small satellite launch vehicle. This vehicle is under development by AirLaunch LLC. This is part of the Force Application and Launch from Continental United States (FALCON) effort.

Active current DARPA projects include:

ACTUV - A project to build an unmanned Anti-submarine warfare vessel.

Adaptive Vehicle Make - Revolutionary approaches to the design, verification, and manufacturing of complex defense systems and vehicles.

ArcLight (missile) - Ship based weapon system that is capable of striking targets nearly anywhere on the globe. It is based on the Standard Missile 3.

Battlefield Illusion

BigDog/Legged Squad Support System - legged robots.

Boeing X-37

Integrated Sensor is Structure

Boomerang (mobile shooter detection system) - an acoustic Gunshot Location Detection System developed by BBN Technologies for detecting snipers on military combat vehicles.

CALO or "Cognitive Assistant that Learns and Organizes" - software

Combat Zones That See - "track everything that moves" in a city by linking up a massive network of surveillance cameras

DARPA XG - technology for Dynamic Spectrum Access for assured military communications

EATR An autonomous tactical robotic system

FALCON

High Energy Liquid Laser Area Defense System

High Productivity Computing Systems

Human Universal Load Carrier battery-powered human exoskeleton

MAHEM Molten penetrating munition

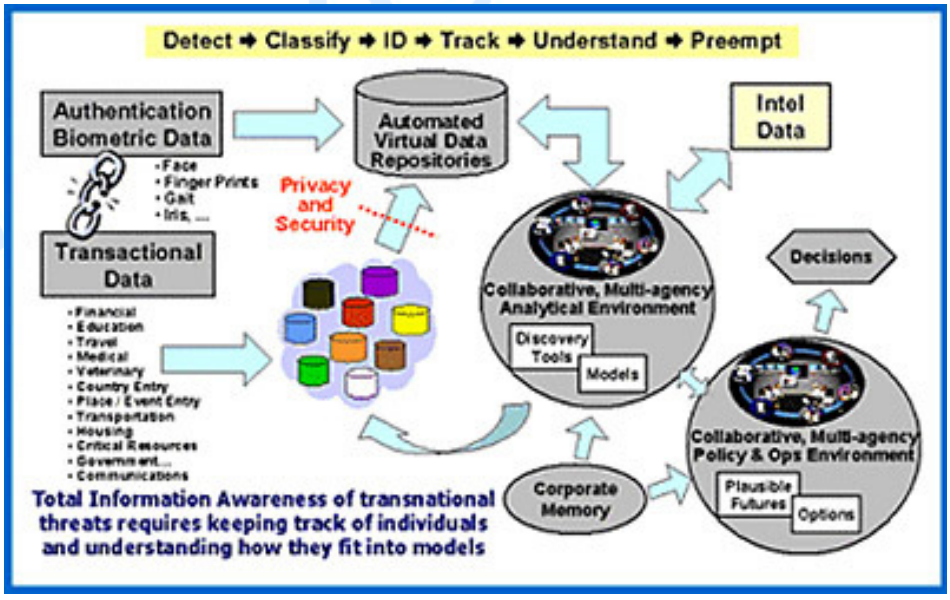
MEMS Exchange MEMS Implementation Environment
MeshWorm, an earthworm-like robot.
Mind's Eye - A visual intelligence system capable of detecting and analysing activity from video feeds.
Persistent Close Air Support
Phoenix - A Satelite project with the aim to recycle retired satelite parts into new on-orbit assets.Launches in 2016.
Protein Design Processes
Proto 2 - a thought-controlled prosthetic arm
Remote-controlled insects
DARPA Silent Talk - A planned program attempting to identify EEG patterns for words and transmit these for covert communications.
Satellite Remote Listening System - a satellite mounted system that can eavesdrop on a targeted area on the surface of the planet in coordination with satellite cameras.[citation needed] This project is in its infant stage.[
SyNAPSE - Systems of Neuromorphic Adaptive Plastic Scalable Electronics
System F6 - Fractionated Spacecraft demonstrator
XOS - powered military exoskeleton
Transformer - flying armoured car
UAVForge
VTOL X-Plane
Vulture
WolfPack

Sister organizations

Advanced Research Projects Agency-Energy (ARPA-E) - Department of Energy
Homeland Security Advanced Research Projects Agency (HSARPA) - Department of Homeland Security
Intelligence Advanced Research Projects Activity (IARPA) - Director of National Intelligence

International equivalents

Defence Science and Technology Laboratory - United Kingdom
Defence Science and Technology Organisation - Australian
Defence Research and Development Canada - Canadian
Tekes - the Finnish Funding Agency for Technology and Innovation - Finland



Total (Terrorist) Information Awareness

After 9/11, the U.S. government began an information stampede to collect any information that might prevent another attack. One of the most ambitious -- and controversial -- plans was a data-mining program known as Total Information Awareness, or TIA. Housed at the Defense Department's

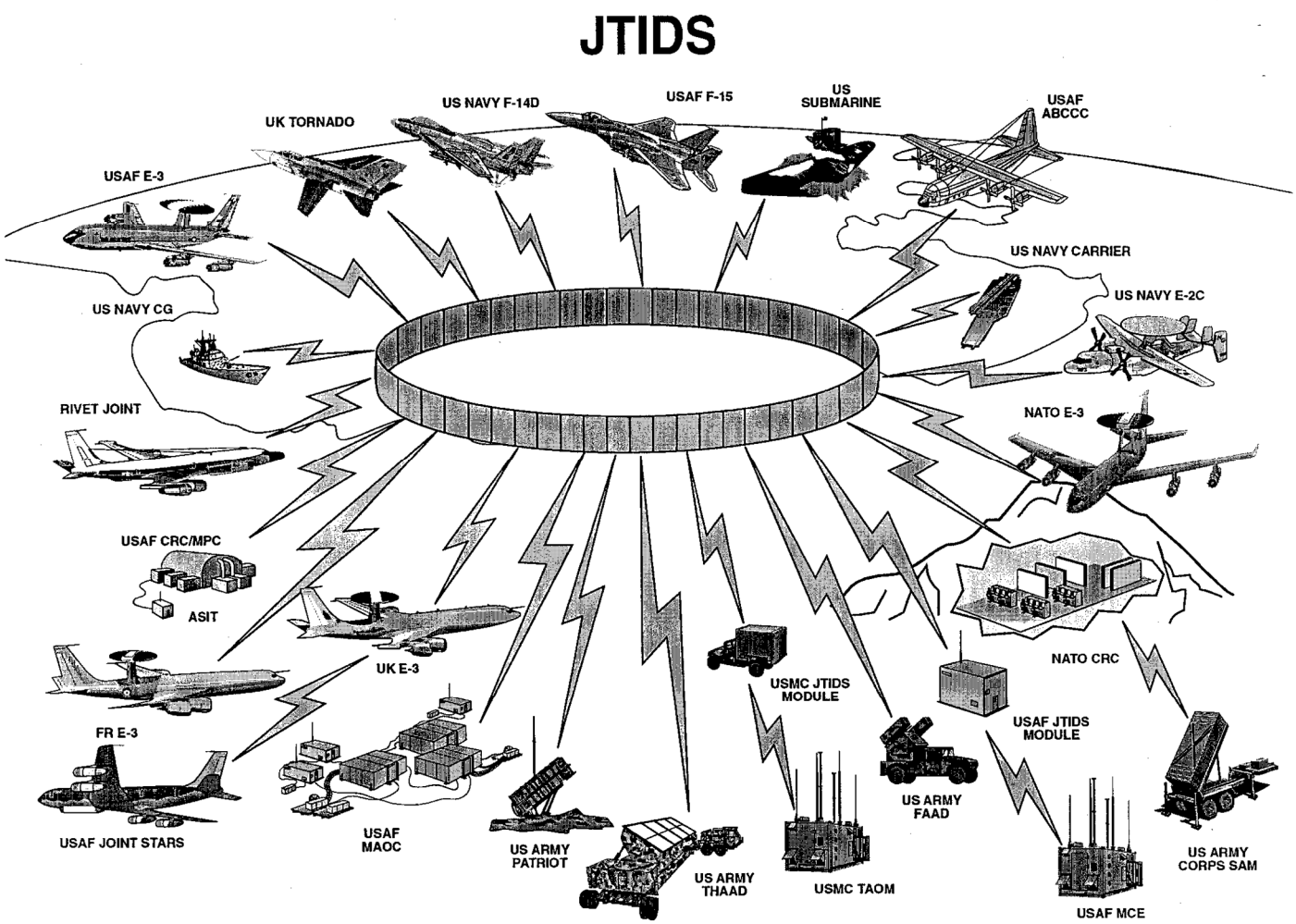
Advanced Research Projects Agency (DARPA) and conceived of by John Poindexter, the former national security adviser to President Reagan known for his involvement in the Iran-Contra scandal, TIA aimed to sift through vast amounts of data to find and pre-empt terrorist plots. An ensuing firestorm in the press over privacy concerns led Congress to kill TIA's funding; however the ultimate effect was to push elements of the program into other agencies, *behind closed doors*.

The IAO's stated mission is to gather as much information as possible about everyone in a centralized location for easy perusal by the United States government, including Internet activity, credit card purchase histories, airline ticket purchases, car rentals, medical records, educational transcripts, driver's licenses, utility bills, tax returns, and any other available data. In essence, the goal of the IAO is to be able to recreate a life history of thoughts and movements for any individual on the planet on demand, which the Bush administration deems necessary to counter the threat of terrorism. Critics claim the very existence of the IAO completely disregards the concept of individual privacy and liberties and is far too invasive and prone to abuse.

The IAO was first mentioned in the media by New York Times reporter John Markoff on February 13, 2002, with few details available as to the agency's role or activities. In the following months, as more and more information emerged about the IAO's full scope, protest among civil libertarians grew over what they claim is the IAO's disturbingly Orwellian mission, especially within the larger framework of other invasive homeland security measures and policies implemented by the Bush administration. Also at issue is the integrity of Poindexter as head of the IAO, as he was convicted on five felony charges for lying to the Congress and deliberately altering and destroying documents pertaining to the Iran-Contra Affair.

On January 16, 2003, US Senator Russ Feingold introduced legislation to halt activity of the IAO and the Total Information Awareness initiative pending a Congressional review of privacy issues involved. A similar measure introduced by Senator Ron Wyden would bar the IAO from operating within the United States unless specifically authorized to do so by Congress, and would shut the IAO down entirely 60 days after passage, unless either the Pentagon prepared a report assessing the impact of IAO activities on individual privacy and civil liberties, or the President certifies that the program's research is vital to national security interests. Any action in the US Congress to attempt to halt a specific internal Department of Defense project is highly unusual, underscoring the grave threat to civil liberties and privacy that many lawmakers perceive in the Information Awareness Office.

Joint Tactical Information Distribution Systems (TIA military)



Name Change & Reprimand lead to agenda change

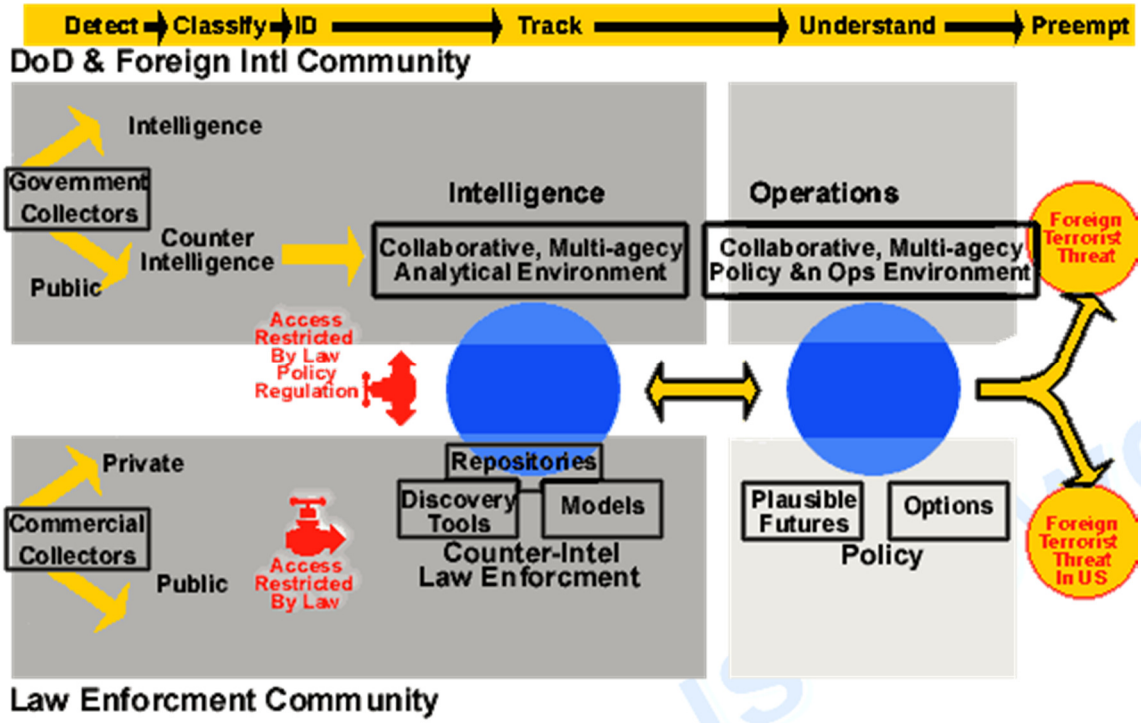
"No government agency may deploy or implement any component of the Terrorism Information Awareness (formerly Total Information Awareness) program without Congressional notification and authorization", according to a provision adopted by the House of Representatives in 2004.

This *"Limitation on Deployment of Terrorism Information Awareness Program"* was included in the *2004 Defense Appropriations Act* that was approved by the House on July 8. (H.R. 2658 Sec. 8124)

The funding was *rejected* via the Conference Report on H.R. 2658, Department of Defense Appropriations Act, 2004 September 24, 2003, House Report 108-283; per the following clauses:

- Sec. 8131. (a) Notwithstanding any other provision of law, none of the funds appropriated or otherwise made available in this or any other Act may be obligated for the Terrorism Information Awareness Program ...
- the term "Terrorism Information Awareness Program" means the program known either as Terrorism Information Awareness or Total Information Awareness, or any successor program, funded by the Defense Advanced Research Projects Agency, or any other Department or element of the Federal Government, including the individual components of such Program developed by the Defense Advanced Research Projects Agency.

Subsequent reviews, stated that the restrictions have been regarded as only for "deployment and implementation", not for research.



Government Quietly Brings Back Total Information Awareness through 'splitting hairs' on the 'research' restrictions

Reuters obtained a Congressional report that shows 9 months after Congress shut down the controversial Pentagon computer-surveillance program called *Total Information Awareness*, the U.S. government continues to comb private records and databases to sniff out suspicious activity. Peter Swire, who served as the Clinton administration's top official said *"I believe that Total Information Awareness is continuing under other names."*—reported by Democracy Now!, June 3, 2004.

This Data Mining has continued thru to current (2013) under the auspice of "research" - with very few "protests" - Even the Democrats that yelled the loudest back in 2002 have barely uttered a peep now.

As part of the IAO's "Total Information Awareness" program, several new technologies are being researched.

- *Effective Affordable Reusable Speech-to-text, or EARS*, has a stated goal of "developing speech-to-text (automatic transcription) technology whose output is substantially richer and much more accurate than currently possible." This program is focusing on broadcast and telephone human conversations in multiple languages, necessary for the computerized analysis of the massive amount of phone tapping the IAO now has the right to perform without a legal warrant.
- *Futures Markets Applied to Prediction, or FutureMAP*, intends to "concentrate on market-based techniques for avoiding surprise and predicting future events." It will analyze data from the world's economy in attempt to predict political instability, threats to national security, and in general every major event in the near future. The IAO's stated strategy for this division includes "the markets must also be sufficiently robust to withstand manipulation," possibly suggesting the intention of altering future events to further the goals of the United States. See prediction market for more detail on the general phenomenon and its relationship to propaganda efforts.
- *Genisys* is the name given to the database system which will be implemented as the center of information for the IAO. Currently used database systems designed in the 1980s are insufficient for the massive amount of data to be gathered.
- *Genoa* "provides the structured argumentation, decision-making and corporate memory to rapidly deal with and adjust to dynamic crisis management." In essence, this program is designed to make conclusions and decisions based on available information, incorporating human analysis, corporate history, and a structured set of thinking. This research project was finished in fiscal year 2002, and is being followed up by Genoa II, which effectively automates the collaboration between government departments.
- *Human Identification at a Distance, or HumanID*, "is to develop automated biometric identification technologies to detect, recognize and identify humans at great distances." This program intends to be able to implement a face and gait identification system effective up to 150 meters at all times by fiscal year 2004. An extreme proposed version of this is called cognotechnology and would rely on nanotechnology.
- *Translingual Information Detection, Extraction and Summarization, or TIDES*, is being developed to detect, translate, summarize, and extract information in speech or text in multiple languages. Demonstration of machine capabilities and integration into Total Information Awareness systems is expected in 2003.
- *Wargaming the Asymmetric Environment, or WAE*, is intended to develop automated technology capable of predicting terrorist attacks, identifying predictive indicators by examining individual and group behavior in broad environmental context. The WAE will also develop intervention strategies based on the motivation of specific terrorists.

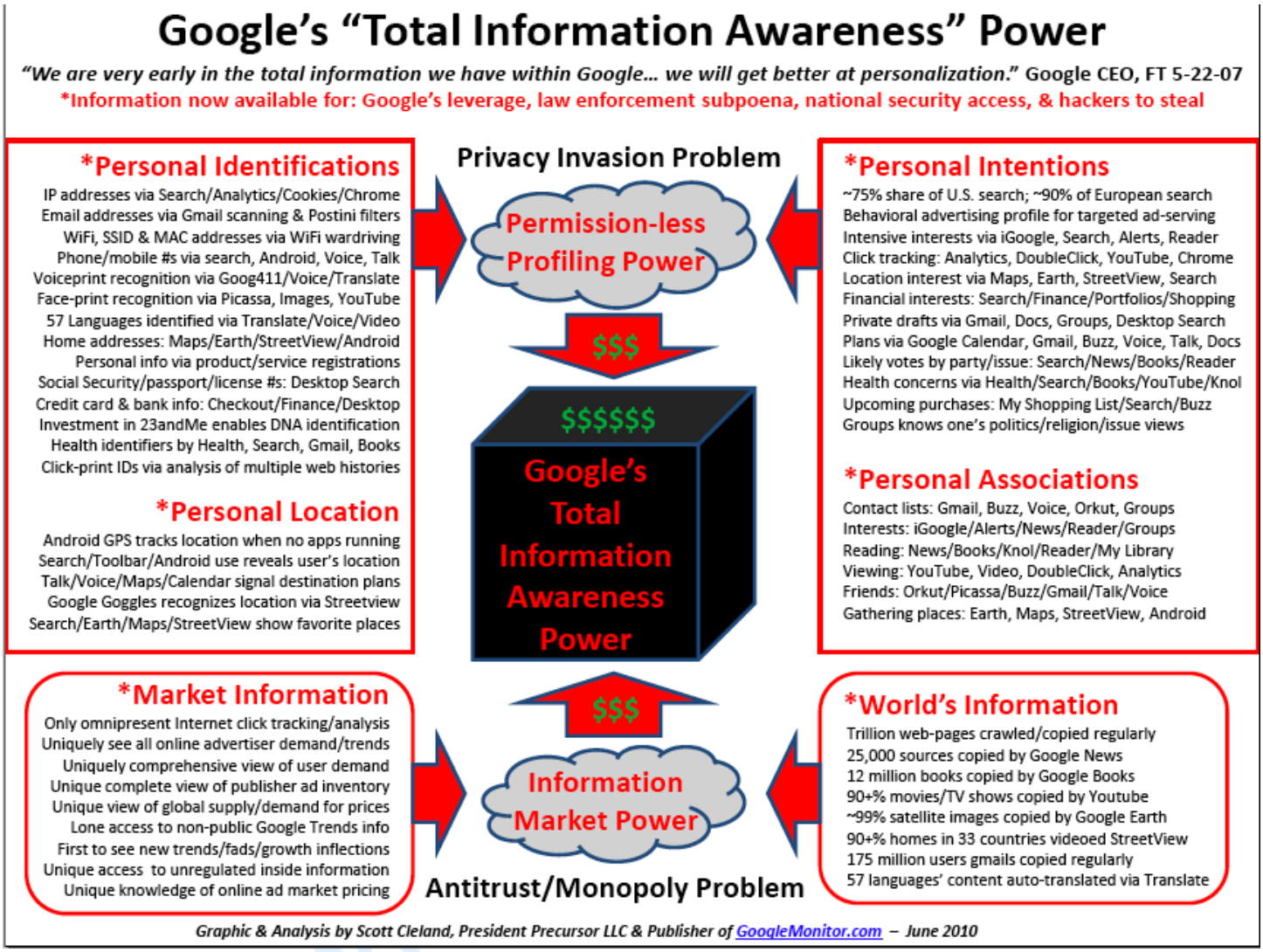
T.I.A. Contractors

- Booz Allen & Hamilton Inc. is the 'integrator' responsible for tying hardware, artificial intelligence, inputs, etc. together.

- "Proposed Projects Under the Information Awareness Office" The Memory Hole: "Projects That Were Accepted and Will Be Funded by IAO."
- Information Links Courtesy of the Electronic Privacy Information Center (EPIC).

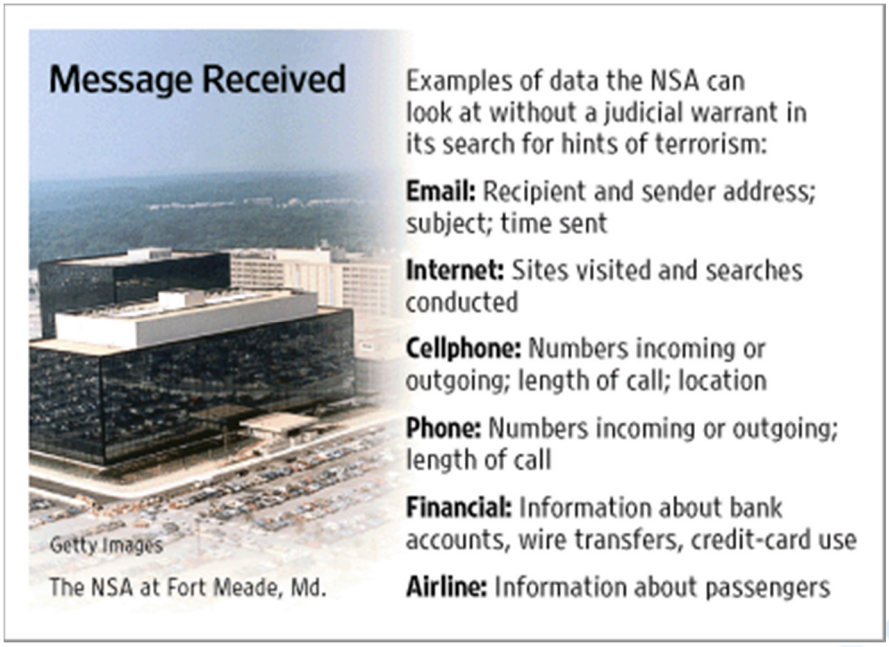
By 2006 other reports of the continuation of TIA in the "*Shadow Government*" made the press. These reports of "*research*" turning into "*live testing*" have increased, *exponentially*, since 2006 to present (2013), in both mainstream and alternative media. Whenever you hear about "*Data Mining*" you are hearing about DARPA and its TIA program. Here are some examples:

- **In May 2007 PBS aired a program called: Pre-Emption - Total Information Awareness - Spying On The Home** (http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/tia.html).
- **What the government's Big Data Initiative was all about? Government Puts $200 Million Behind Big Data Initiative March 30, 2012** http://www.datanami.com/datanami/2012-03-30/government_puts_$200_million_behind_big_data_initiative.html
- **'Total Information Awareness' surveillance program returns, bigger than ever March 16, 2012** http://www.rawstory.com/rs/2012/03/16/total-information-awareness-surveillance-program-returns-bigger-than-ever/
- **Seven Big Winners in the U.S. Big Data Drive April 05, 2012** http://www.datanami.com/datanami/2012-04-05/7_big_winners_in_u.s._big_data_drive.html
- **Total Information Awareness: Sweeping New Surveillance Measures Approved in the US. Friday, 23 March 2012** http://truth-out.org/news/item/8067-total-information-awareness-sweeping-new-surveillance-measures-approved-in-the-us
- **World's Top Data-Intensive Systems Unveiled June 22, 2012** http://www.datanami.com/datanami/2012-06-22/world_s_top_data-intensive_systems_unveiled.html
- **U.S. Relaxes Limits on Use of Data in Terror Analysis March 22, 2012** http://www.nytimes.com/2012/03/23/us/politics/us-moves-to-relax-some-restrictions-for-counterterrorism-analysis.html?_r=3&
- **How DARPA Does Big Data August 15, 2012** http://www.datanami.com/datanami/2012-08-15/how_darpa_does_big_data.html

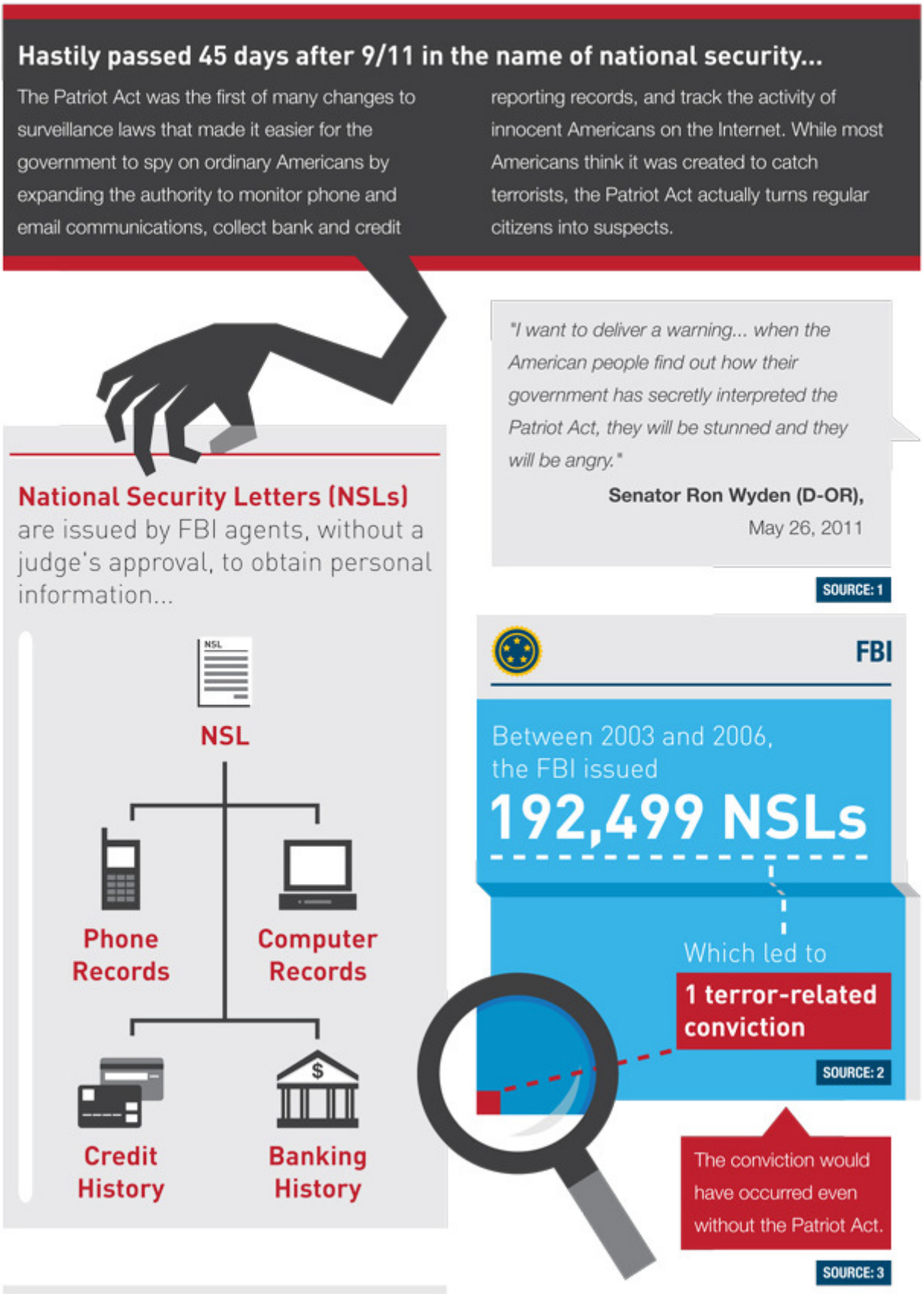


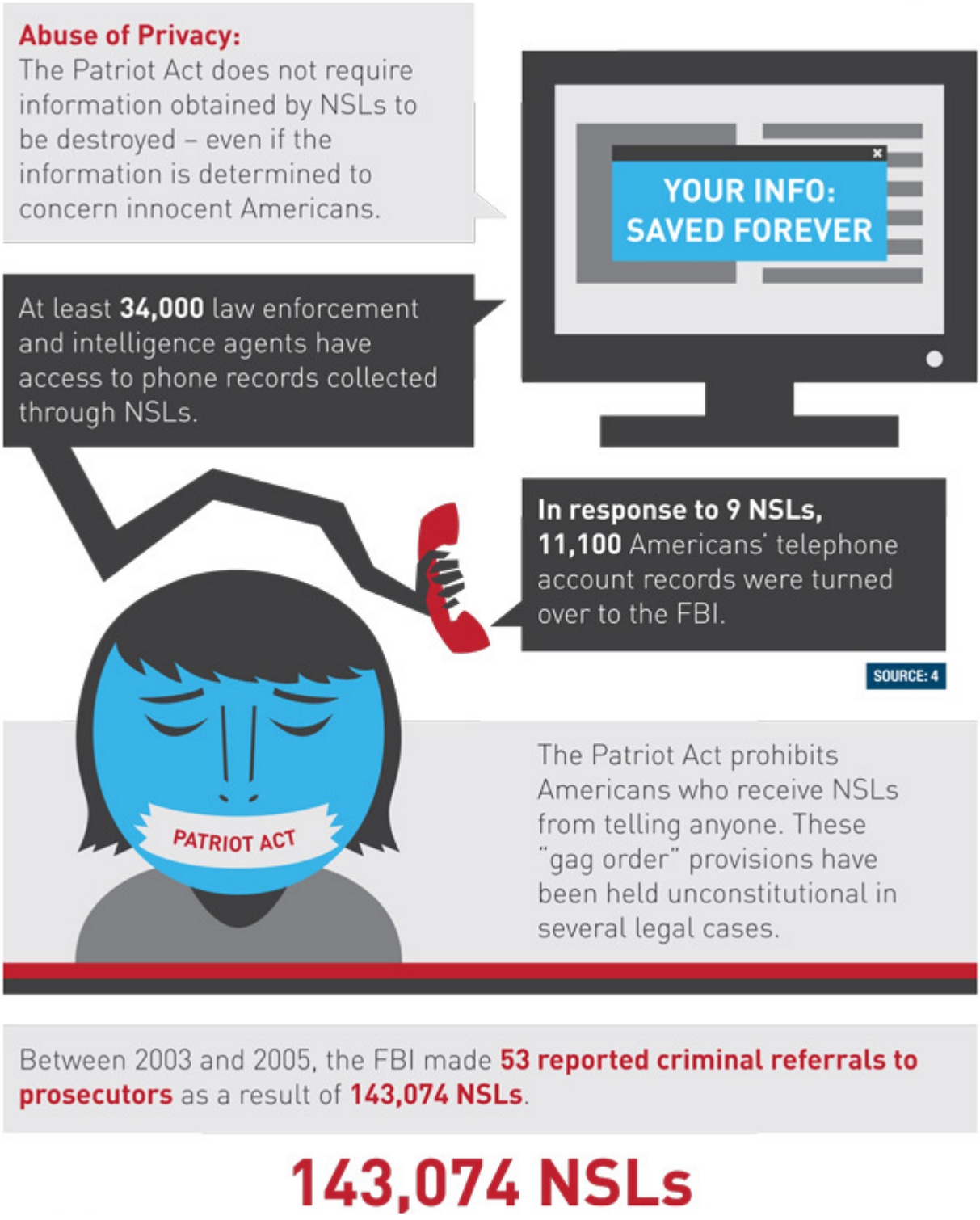
For technical information on your electronic privacy, and the invasion of it see Electronic Frontier Foundation https://www.eff.org/ and Electronic Privacy Information Center www.EPIC.org.

What NSA Can Look At WITHOUT a Judicial Warrant



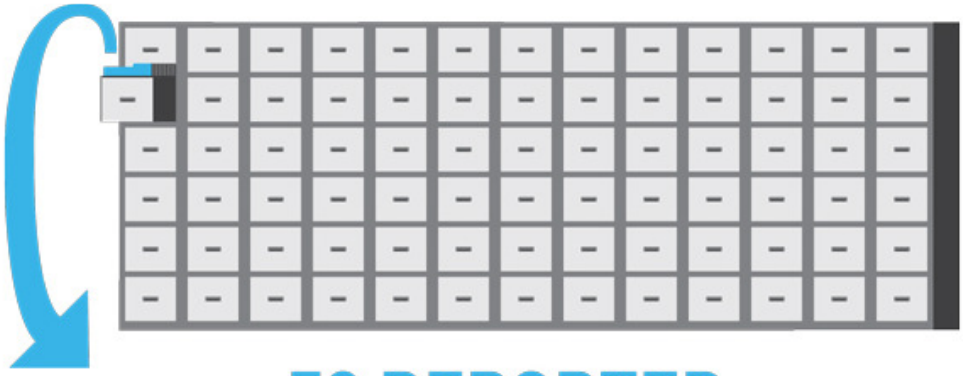
The Patriot Act (October 26, 2001) created changes to many DARPA directives, some rescinded, many more continue to this day (2013) …


Hastily passed 45 days after 9/11 in the name of national security...
The Patriot Act was the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit reporting records, and track the activity of innocent Americans on the Internet. While most Americans think it was created to catch terrorists, the Patriot Act actually turns regular citizens into suspects.
National Security Letters (NSLs) are issued by FBI agents, without a judge's approval, to obtain personal information...
NSL
Phone Records
Computer Records
Credit History
Banking History
"I want to deliver a warning... when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."
Senator Ron Wyden (D-OR), May 26, 2011
SOURCE: 1
FBI
Between 2003 and 2006, the FBI issued
192,499 NSLs
Which led to
1 terror-related conviction
SOURCE: 2
The conviction would have occurred even without the Patriot Act.
SOURCE: 3

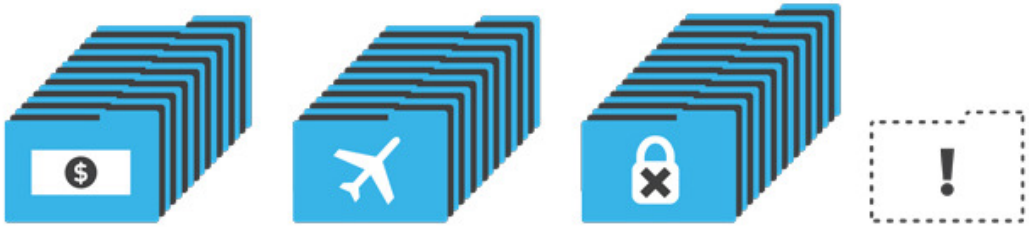


Between 2003 and 2005, the FBI made **53 reported criminal referrals to prosecutors** as a result of **143,074 NSLs**.

143,074 NSLs



53 REPORTED CRIMINAL REFERRALS:



17 were for **MONEY LAUNDERING**

17 related to **IMMIGRATION**

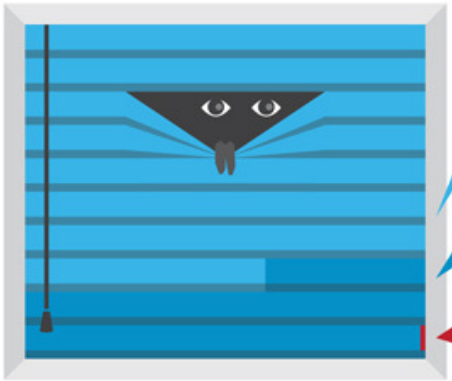
19 involved **FRAUD**

0 were for **TERRORISM**

SOURCE: 5

"Sneak & Peek" Searches:

The Patriot Act allows federal law enforcement agencies to delay giving notice when they conduct secret searches of Americans' homes and offices—a fundamental change to Fourth Amendment privacy protections and search warrants. This means that government agents can enter a house, apartment or office with a search warrant when the occupant is away, search through his/her property and take photographs—in some cases seizing property and electronic communications—and not tell the owner until later.



Of the **3,970 Sneak & Peeks in 2010:**

76% drug-related

24% other

<1% terror-related

SOURCE: 6

Then of course there are the **FBI Fusion Centers**.

A fusion center is an information sharing center, many of which were jointly created between 2003 and 2007 under the *U.S. Department of Homeland Security* and the *Office of Justice Programs* in the U.S. Department of Justice.

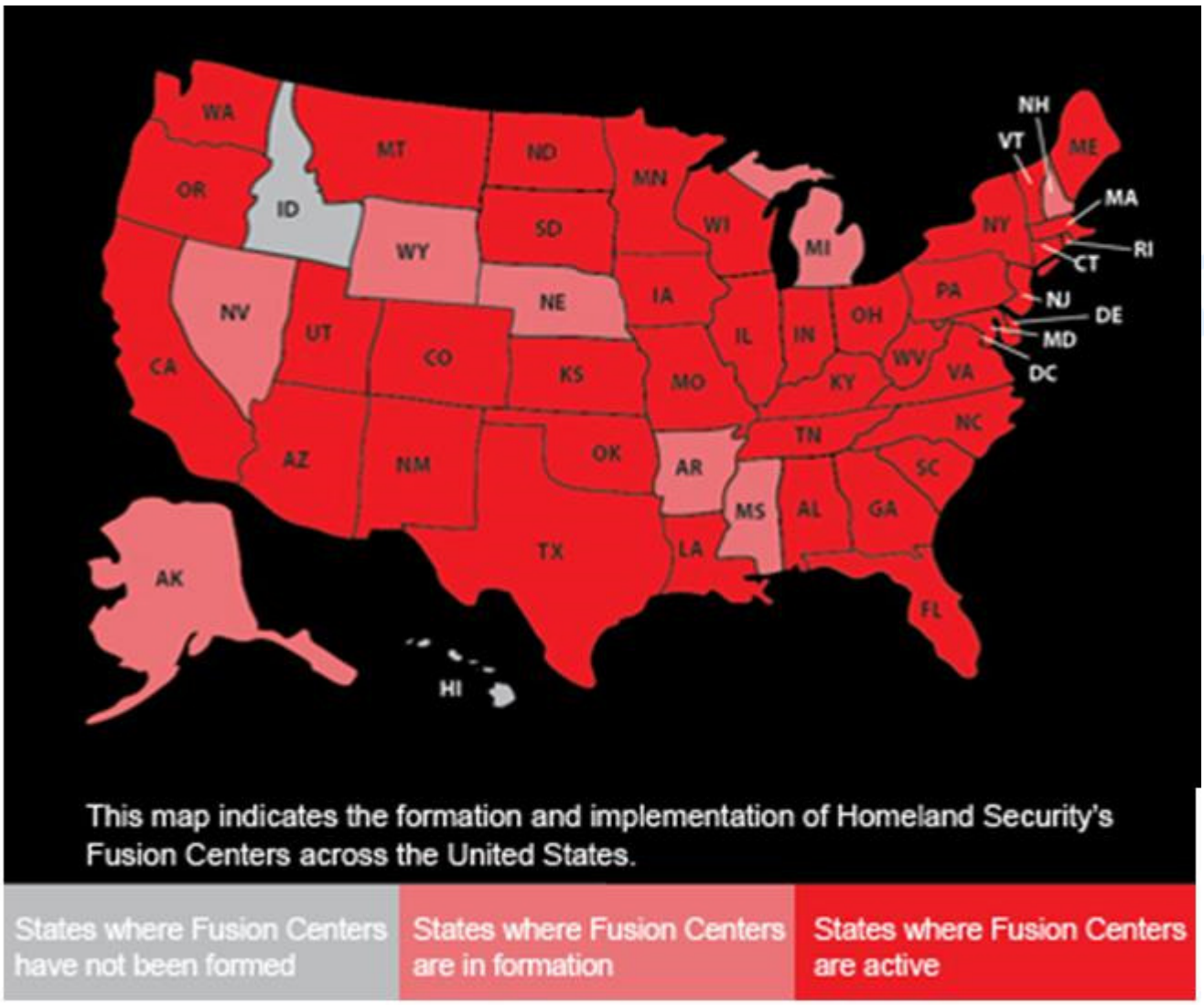
They were designed to promote information sharing at the federal level between agencies such as the *Central Intelligence Agency (CIA)*, *Federal Bureau of Investigation (FBI)*, *U.S. Department of Justice, U.S. military, and state- and local-level government*.

As of July 2009, the U.S. Department of Homeland Security recognized at least 72 fusion centers. Fusion centers may also be affiliated with an *Emergency Operations Center* that responds in the event of a disaster.

The fusion process is an overarching method of managing the flow of information and intelligence across levels and sectors of government to integrate information for analysis. That is, the process relies on the active involvement of state, local, tribal and federal law enforcement agencies—and sometimes on non–law enforcement agencies (e.g., private sector & InfraGard) – to provide the input of raw information for intelligence

analysis. As the array of diverse information sources increases, there will be more accurate and robust analysis that can be disseminated as intelligence.

A two-year senate investigation found that "*the fusion centers often produced irrelevant, useless or inappropriate intelligence reporting to DHS, and many produced no intelligence reporting whatsoever*." Yet they continue to be active.



2012

InfraGard (https://www.infragard.net/) is a non-profit organization serving as a public-private partnership between *U.S. businesses* and the *Federal Bureau of Investigation*. The organization describes itself as an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members.

InfraGard is an association of individuals that facilitates information sharing and intelligence between *businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to prevent hostile acts against the United States*. InfraGard's mutual nondisclosure agreements among its members (individuals) and the FBI promotes trusted discussions of vulnerabilities and solutions that companies and individuals may be hesitant to place in the public domain.

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI sponsored program and will work with DHS in support of its CIP mission, facilitate InfraGard's continuing role in CIP activities, and further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

Since 2003, InfraGard Alliances and the FBI said that they have developed a TRUST-based public-private sector partnership to ensure reliability and integrity of information exchanged about various terrorism, intelligence, criminal, and security matters. It supports FBI priorities in the areas of counterterrorism, foreign counterintelligence, and cybercrime.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of indiviudals, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The relationship supports information sharing at national and local levels and its objectives are as follows:

- Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs.
- Increase interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.
- Provide members value-added threat advisories, alerts, and warnings.
- Promote effective liaison with local, state and federal agencies, to include the Department of Homeland Security.
- Provide members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interest.

InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

Each FBI Field Office has a Special Agent Coordinator who gathers interested individuals to form a chapter. Any individual can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. The following illustrates additional activities that local chapters may offer:

- Training and education initiatives
- A local newsletter
- A Contingency Plan for using alternative systems in the event of a successful large scale attack on the information infrastructure

InfraGard members are represented nationally by an elected board of seven representatives called the InfraGard Board of Directors. Elections are held annually at the InfraGard National Congress for voluntary two-year terms. The Board is responsible for representing the membership in the partnership with the FBI. They conduct weekly conference calls to address a variety of issues that face the organization. Board members travel to various chapter activities and attend conferences promoting InfraGard and other issues pertinent to the program.

The Board established several committees to address issues such as membership, incorporation, and partnerships with other private sector association / organizations.

Special Interest Groups (SIGs) have also been established to meet the challenges America faces in protecting against criminal, terrorist, and intelligence threats. One such SIG involves InfraGard, the National Institute of Standards and Technology (NIST), the Small Business Administration, and the FBI.

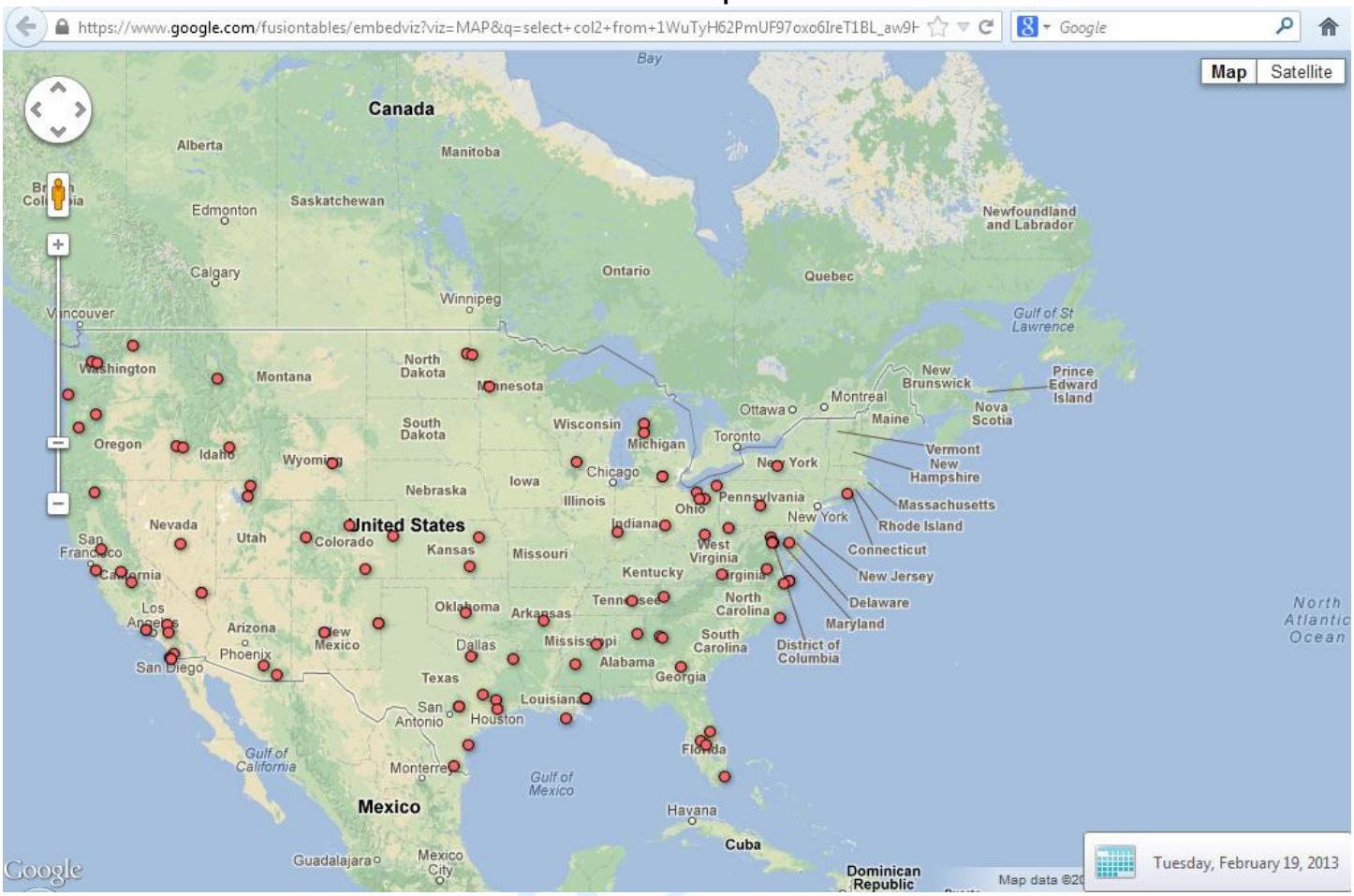
The information sharing between the organization and government has been criticized by those protecting civil liberties, concerned the membership would be surrogate eyes and ears for the FBI. The group has also been the subject of hacking attacks intended to embarrass the FBI. Local chapters regularly meet to discuss the latest threats or listen to talks from subject matter experts on security issues, with membership open to U.S. citizens at no cost.

As of March, 2013, the organization reported membership at over 54,677 (including FBI).

Drones are another surveillance method now deployed in the U.S. as well as other countries "*to protect the United States from terrorism*". They have been around awhile, however here are a few of the more recent reports:

Are Drones Watching You? January 10, 2012 https://www.eff.org/deeplinks/2012/01/drones-are-watching-you
FAA Makes Progress with UAS Integration of Drones via the National Airspace System (NAS) 05/14/12
http://www.faa.gov/news/updates/?newsId=68004
EFF Demands Answers About Predator Drone Flights in the U.S. October 31, 2012 https://www.eff.org/press/releases/eff-demands-answers-about-predator-drone-flights-us
The solar-powered spy plane that will be able to fly non-stop for FIVE years September 20, 2010
http://www.dailymail.co.uk/sciencetech/article-1313552/The-solar-powered-spy-plane-able-fly-non-stop-FIVE-years.html
FAA Releases Lists of Drone Certificates—Many Questions Left Unanswered Apr 2012
https://maps.google.com/maps/ms?msa=0&msid=214769660919529725423.0004bde31d74fe6eb1ece&hl=en&ie=UTF8&t=m&ll=45.336702,-110.039062&spn=58.987964,112.5&z=3&source=embed
In Brooklyn Nautical Drones Explore Troubled Waters Sep 14 2012 http://us2.campaign-archive1.com/?u=5b63a0823e3b9c105434c46d7&id=0ed24a86a4&e=35c67c69a1
Drones tested as tools for police and firefighters August 5, 2012 http://www.latimes.com/news/nationworld/nation/la-na-drones-testing-20120805,0,6483617.story
UAV update Drones used by police, firefighters raise privacy concerns August 8, 2012
http://www.homelandsecuritynewswire.com/dr20120808-drones-used-by-police-firefighters-raise-privacy-concerns
Homeland Security Learns to Love Small Spy Drones 10/8/2012 http://www.nationalterroralert.com/2012/10/08/homeland-security-learns-to-love-small-spy-drones/ & http://www.wired.com/dangerroom/2012/10/robotic-aircraft-public-safety/

Domestic Drone Requests 2013



FAA Releases New Drone List—Is Your Town on the Map? February 7, 2013 https://www.eff.org/deeplinks/2013/02/faa-releases-new-list-drone-authorizations-your-local-law-enforcement-agency-map

Drone Flights in the US-2012 FAA List of Drone License Applicants Feb 2013
https://www.eff.org/sites/default/files/filenode/faa_coa_list-2012.pdf

Justice Department memo reveals legal case for drone strikes on Americans Feb 4 2013
http://openchannel.nbcnews.com/_news/2013/02/04/16843014-justice-department-memo-reveals-legal-case-for-drone-strikes-on-americans?lite

DOJ Drone Strikes on Americans White Paper Feb 4 2013
http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf

Rise of the Drones Aired January 23, 2013 on PBS http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html

Could the Pentagon's 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance? Feb. 6, 2013
http://www.slate.com/blogs/future_tense/2013/02/06/argus_is_could_the_pentagon_s_1_8_gigapixel_drone_camera_be_used_for_domestic.html

The U.S. Drone Census https://www.muckrock.com/drone-census/ (Want to know if a particular agency has plans for using drones, or what their drone policies are? To submit your own public records request and help build the Drone Census database see https://www.muckrock.com/news/archives/2012/jul/03/drone-watch-help-eff-and-muckrock-uncover-planned-/#file)

Pentagon's 1.8 Gigapixel Drone Camera Jan 2013

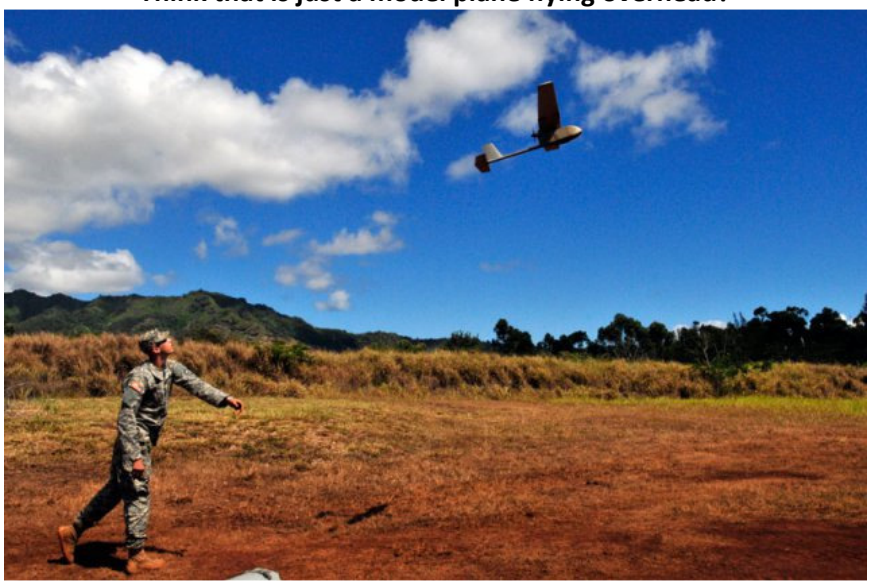
The ARGUS-IS mission poster. Image courtesy DARPA

Now on top of all of this type of surveillance don't forget:

- In store camera's to help prevent shoplifting
- ATM cameras that also see the road or parking lot in front of the ATM
- Parking lot cameras that are to prevent auto break-ins, theft and parking lot muggings
- Toll booth cameras that capture the driver and license of the vehicle at the toll booth
- Traffic cameras in major cities and high traffic highways to aid in re-routing traffic to avoid congestion
- A few US cities, many EU countries (especially the UK) have pedestrian cameras to reduce street crime
- Businesses and Schools have cameras in their buildings and parking lots for a multitude of so called "safety and espionage" reasons
- Transportation centers (airports, bus stations and or stops, train and subway stations, ferry stations, etc) have cameras for a number of reasons

Some of these "reason" are good or have a valid basis to them, others are not; ALL are dangerous because there is NO checks & balances in place to prohibit and restrict inappropriate use by an operator, employee or government entity.

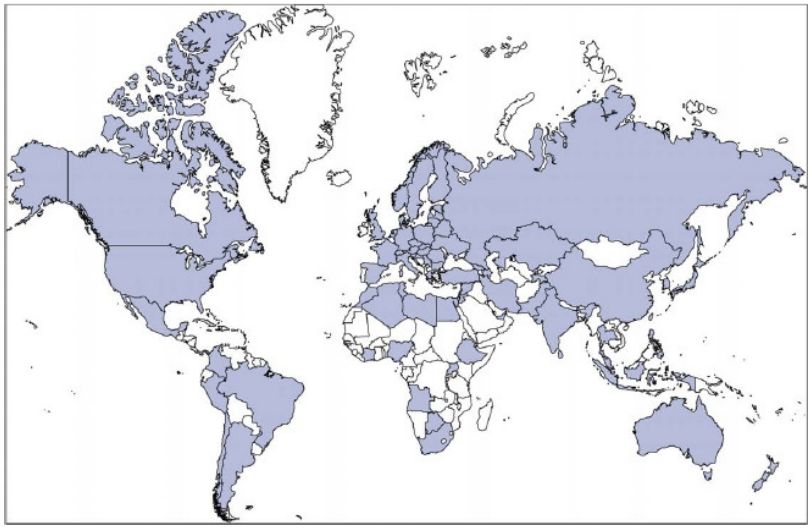
Think that is just a model plane flying overhead?



Better think again!

Of course we also have GPS, GIS and Geo Tagging surveillance.

Countries that have drones according to GAO report



The US [Government Accountability Office (GAO) has published an unclassified version of its February 2012 report on the proliferation of UAVs](http://dronewarsuk.files.wordpress.com/2012/09/us-gao-_-noproliferation-of-uavs.pdf) (http://dronewarsuk.files.wordpress.com/2012/09/us-gao-_-noproliferation-of-uavs.pdf & http://dronewarsuk.files.wordpress.com/2012/09/world-drone-map2.jpg)