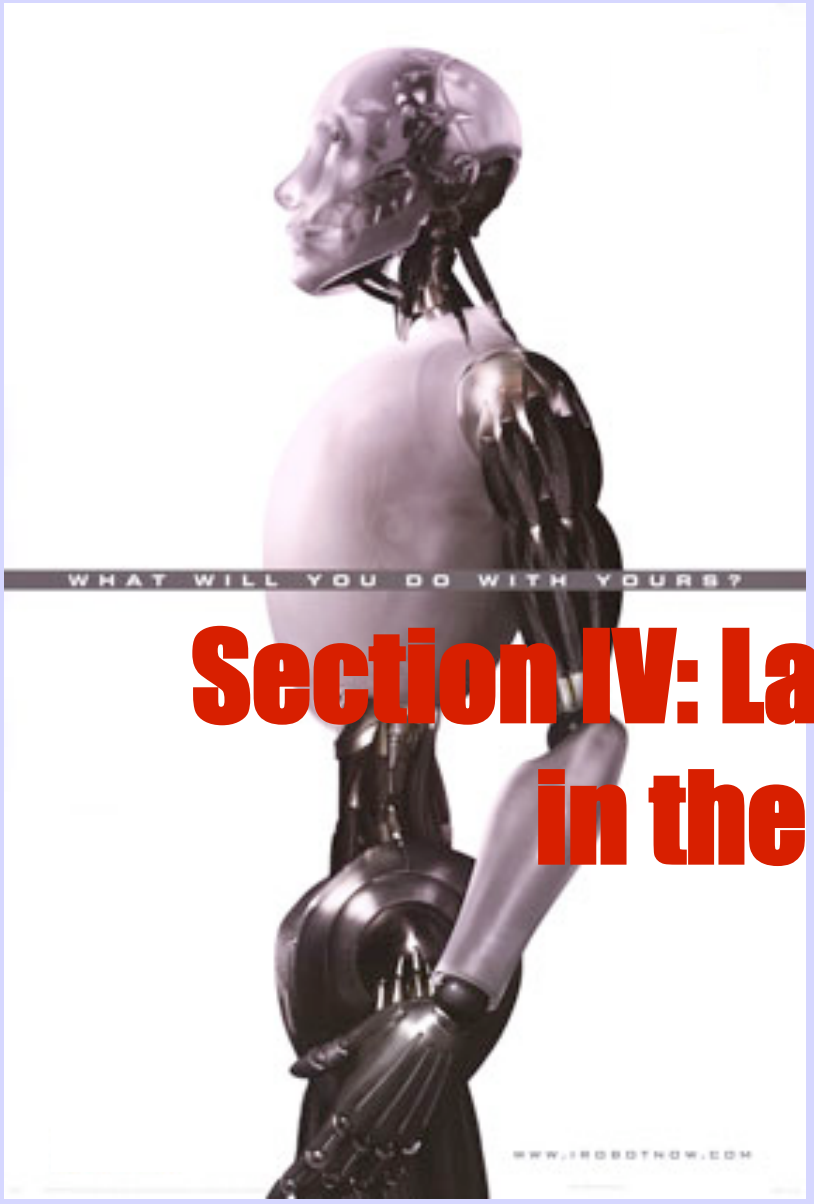


Section IV: Law and Civil Liberty in the Digital Age

Lecture Outline

1. Laws dealing with Digital Issues
    a. Patriot Act
    b. DMCA
    c. Intellectual Property
2. Technology and Civil Liberties
    a. TIA
    b. Surveillance
    c. “Big Picture”

Law in the Digital Age

This section will discuss some of the laws enacted to deal with new crimes involving technology and its use.

Many of the new laws deal with copyright issues and search and seizures.

1. Patriot Act
2. DMCA
3. Intellectual Property

U.S. Patriot Act

Subtitled:

Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism.

Purpose of Bill:

To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

Main Components of Patriot Act

Title I: Enhancing Domestic Security Against Terrorism

Requires the Director of the Secret Service to develop a national network of electronic crime task forces throughout the U.S. to prevent, detect, and investigate various forms of electronic crimes.

Allows the President, when the U.S. is engaged in armed hostilities or has been attacked by foreign nationals, to confiscate any property subject of a foreign person, organization, or country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks.

Title II: Enhanced Surveillance Procedures

Amends the federal criminal code to authorize the interception of wire, oral, and electronic communications for the production of evidence of (1) specified chemical weapons or terrorism offenses, and (2) computer fraud and abuse.

**Basically makes it easier for the government to gather and share information on suspected terrorist. Lowers standards for wire, oral or electronic wiretapping.

Title III: International Money laundering Abatement and Anti-Terrorism Financing Act

Amends federal law to revise requirements for civil liability immunity for voluntary financial institution disclosure of suspicious activities. Authorizes the inclusion of suspicions of illegal activity in written employment references.

Amends the Right to Privacy Act to permit the transfer of financial records to other agencies or departments upon certification that the records are relevant to intelligence or counterintelligence activities related to international terrorism.

Amends the fair Credit Reporting Act to require a consumer reporting agency to furnish all information in a consumer's file to a government agency upon certification that the records are relevant to intelligence or counterintelligence activities related to international terrorism.

Title IV: Protecting the Border

Provides for mandatory detention until removal from the U.S. of an alien certified by the Attorney General as a suspected terrorist or threat to national security. Limits judicial review to Habeas Corpus proceedings in the U.S. Supreme Ct., The U.S. Ct. of Appeals for D.C. or any district ct. with jurisdiction to entertain a habeas corpus petition.

Changes the definition of Terrorist and Terrorist Organization: Group designation under the Immigration and Nationality Act by Secretary of State OR a group of two or more people, related or otherwise, which engage in terrorist –related activities.

Also expanded the list of "terrorist related actions"

Title V: Removing Obstacles to Investigating Terrorism

Allows the FBI to request telephone toll and transactional records, financial records, and consumer reports in any investigation to protect against international terrorism or clandestine intelligence activities only if the investigation is not conducted solely on the basis of activities protected by the first amendment.

Title VI: Providing for Victims of Terrorism, Public Safety Officers, and Their Families.

Provides expedited payments to those whose family members were killed during the terrorist attack.

Title VII: Increased Information Sharing for Critical Infrastructure Protection

Increases federal funding for the creation and enhancement of databases that share information across local, state, and federal jurisdictions.

Title VIII: Strengthening the Criminal Laws Against Terrorism

Changes some of the definitions of terrorism under federal criminal law and adds some new actions.

Aspects of Patriot Act related to Technology

Several of the sections of the Patriot Act have an explicit impact on technology and the use of technology by Police to investigate crime.

This section of the lecture will review some of the Sections of the Patriot Act that deal explicitly with technology.

1. Section 201: Wiretapping (General)
2. Section 202: Wiretapping related to computer crime.
3. Section 206: Roving Surveillance
4. Section 209: Voicemail Seizures
5. Section 212: Emergency Disclosure of Electronic Communications
6. Section 214: Pen registers and tap and trace
7. Section 220: Nationwide Search Warrants for Electronic Evidence
8. Section 223: Civil Liability for Unauthorized Disclosure

Section 201: Wiretapping

This section makes it so the FBI can get a wiretap to listen in on your private conversations based on your association with an organization classified by the U.S. government as "terrorist" -- whether or not the organization engages in legitimate political advocacy or humanitarian work.

An example of such an organization is the anti-apartheid African National Congress, which was designated a "terrorist" organization before apartheid was defeated.

The FBI can wiretap your phone, or "bug" your house or office, only when investigating the most serious crimes. PATRIOT 201 made a number of additions to the list of crimes that can justify police surveillance, including one brand new crime created by PATRIOT Section 805 -- providing "material support" to terrorist organizations in the form of "expert advice or assistance."

Section 201: Wiretapping

Section 805 makes it a crime to offer "expert advice and assistance" to any foreign organization that the Secretary of State has designated as "terrorist."

Many of these "terrorist" organizations also advocate for, and provide humanitarian assistance to, their constituents. Yet PATRIOT makes it illegal to offer expert advice and assistance even for these legal, non-terrorist activities.

Importantly, HAMAS, which is now the ruling party of Palestine is still designated as a terrorist group. Thus any individual who provides ANY expert advice or assistance to HAMAS on how to run the country or any aspect of the government could be considered aiding a terrorist organization.

One federal court has already ruled that PATRIOT Section 805 is unconstitutional, since the vague terms "expert advice and assistance" could criminalize the First Amendment-protected activities described above. Yet the law is still in force throughout most of the U.S.

Section 202: Wiretapping relating to Computer Crime

This Section makes it easier for the FBI to get privacy-invasive wiretap orders and to intercept your electronic communications when investigating computer crimes even when those crimes have absolutely nothing to do with terrorism.

The Justice Department persuaded Congress to expand the government's wiretap powers without ever having to cite even a single instance in which a computer-crime investigation - much less a terrorism investigation - had been hindered due to lack of surveillance authority.

The Justice Department also succeeded in pushing through a provision that under some circumstances gives the FBI the power to intercept your private electronic communications - email messages, faxes, instant messages, etc. - without a judge's approval.

Section 202: Wiretapping relating to Computer Crime

Section 202: The FBI can get a court's authorization to "bug" face-to-face conversations or tap phone calls only when investigating especially serious crimes.

PATRIOT added computer crime to the list of felonies that justify such profound violations of privacy- despite the fact that the Justice Department never presented evidence to suggest that this is necessary in the battle against either computer crime or terrorism.

Section 217: It used to be that in order to intercept your private electronic communications in a computer-crime investigation, the FBI had to seek permission from a court.

No more. Now, so long as a computer service provider merely claims you are "trespassing" on its network, the FBI is free to intercept your private communications as it so chooses.

Section 206: Roving Surveillance

Section 206 authorizes intelligence investigators to conduct "John Doe" roving surveillance - meaning that the FBI can wiretap every single phone line, mobile communications device or Internet connection that a suspect ***might*** be using, without ever having to identify the suspect by name.

This gives the FBI a "blank check" to violate the communications privacy of countless innocent Americans. What's worse, these blank-check wiretap orders can remain in effect for up to a year.

Imagine that the FBI could, with a single search warrant, raid every house or office that an individual suspect has visited over an entire year - every single place, whether or not the residents themselves are suspects. Suppose that the FBI could do this without ever having to identify the suspect in question.

This is basically what Section 206 allows

Section 206: Roving Surveillance

Section 206 amended the Foreign Intelligence Surveillance Act (FISA) so that a wiretap order issued by the secret FISA court no longer has to specify what type of communications that the order applies to.

This allows investigators to engage in "roving" surveillance, using a single wiretap order to listen in on any phone line or monitor any Internet account that a suspect may be using - whether or not other people who are not suspects also regularly use it.

FISA wiretaps lack many of the safeguards that prevent abuse of criminal wiretaps. For example, orders are issued using a lower legal standard than the "probable cause" used in criminal cases, are subject to substantially less judicial oversight and typically last at least three times longer than criminal wiretaps.

Surveillance targets are never notified that they were spied on. Most important, and also unlike criminal wiretaps, the FISA court can issue "John Doe" wiretaps that don't even specify the surveillance target's name.

Section 209: Voicemail Seizures

Before PATRIOT, the privacy of your voice mail was protected by the Wiretap Act. This meant that in order to listen to your messages, the FBI had to secure a wiretap order.

After PATRIOT, however, your voice mail is governed by the Electronic Communications Privacy Act (ECPA), a statute that gives you much less legal protection against government spying. Now, instead of needing a wiretap order to listen to your voice mail, the FBI can use other legal processes with weaker privacy-protection standards:

- If you haven't listened to your voice mail messages and they are 180 days old or less, the FBI can use a search warrant.
- If you have listened to your messages, or if they are older than 180 days, the FBI can use a special court order for stored communications, or a subpoena.
- In some cases, the FBI may be able to simply ask for the voice mail, and your phone company may give it, without fulfilling any legal requirements at all.

Section 209: Voicemail Seizures

Before PATRIOT, the FBI could gain access to your voice mail only by showing facts to a judge that demonstrate "probable cause" to believe that you are committing a crime.

NOW it need only demonstrate "reasonable grounds" for the search to get a court order -- or, if it uses a subpoena, mere "relevance" to an investigation.

Before PATRIOT, the FBI eventually had to notify you if it listened to your voice mail messages.

NOW if they use a search warrant, the only way you'll find out is if the FBI uses your voice mail against you in court.

Before PATRIOT, the FBI could listen to your voice mail only if you were suspected of one of a limited number of serious crimes.

NOW it can gain access to your voice mail messages for any kind of criminal investigation whatsoever.

Before PATRIOT, if the FBI listened to your voice mail illegally, it couldn't use the messages as evidence against you -- this is the so-called exclusionary rule. But the ECPA has no such rule, so even if the FBI gains access to your voice mail in violation of the statute, it can freely use it as evidence against you.

Section 212: Emergency Disclosure of Electronic Communications

PATRIOT Section 212 allows your ISP or phone company to share your private communications with the government even if it isn't served with a search warrant. This tramples on your rights by allowing the Department of Justice to do an end-run around laws that safeguard the privacy of your personal communications.

Before PATRIOT, in order to get communications records or stored communications -- such as email or voice mail -- from your ISP or phone company, the FBI had to get a search warrant or court order from a judge, or get a subpoena from a grand jury.

Congress gave us this protection in the Electronic Communications Privacy Act of 1986 because even though your ISP or phone company stores messages for you, they're still your messages. They shouldn't be shared without your consent unless a court or grand jury demands them.

Section 212: Emergency Disclosure of Electronic Communications

After PATRIOT Section 212, your ISP or phone company could hand over your private records and messages to any law enforcement agent, so long as that communications provider *reasonably believed* that the immediate danger of death or serious physical injury required it to do so. This could be done without your knowledge or consent.

The Homeland Security Act expanded the power of PATRIOT Section 212 by 1) lowering the relevant standard from "reasonable belief" of a life-threatening emergency to a "good faith belief," 2) allowing communications providers to use the emergency exception to disclose your data to any government entity, not just law enforcement, and 3) dropping the requirement that the threat to life or limb be immediate. Most significantly, HSA Section 225 does not expire, rendering the sunset of PATRIOT Section 212 irrelevant.

Section 214: Pen Registers and Tap and Trace

Section 214 significantly expands the FBI's electronic surveillance powers under the Foreign Intelligence Surveillance Act (FISA), as well as lowering the standards under which the secret FISA court can authorize the FBI to spy on your phone and Internet communications.

In particular, Section 214 makes it easier for the FBI to install "pen registers" and "trap-and-trace devices" (collectively, "pen-traps") in order to monitor the communications of citizens who are not suspected of any terrorism or espionage activities.

Section 214: Pen Registers and Tap and Trace

Before the PATRIOT Act, the government could only get a FISA pen-trap order when the communications to be monitored were likely to be either (1) those of an international terrorist or spy or (2) those of a foreign power or its agents relating to the criminal activities of an international terrorist or spy.

PATRIOT 214 threw out this requirement. Now, any innocent person's communications can be tapped with a pen-trap so long as it is done "for" an intelligence investigation.

The FBI doesn't have to demonstrate to the FISA court that the communications are relevant to its investigation. Nor can the court deny the FBI's request; if the FBI certifies the tap is "for" such an investigation, the FISA court ***must issue*** the order.

Section 214: Pen Registers and Tap and Trace

Before PATRIOT, the statute defined pen registers and trap-and-trace devices solely in the context of telephone communications.

Section 214 expanded the pen-trap definition to include devices that monitor Internet communications, without clarifying what portions of Internet communications are "content," requiring a full wiretap order, versus "non-content," which can be legally acquired only with a pen-trap order.

At the very least, this change means that the government can use a pen-trap to see the email addresses of people you're sending email to and the addresses of people who send email to you, along with the timestamp and size in bytes of each email.

The FBI can monitor the IP addresses of all the computers you interact with over the Internet, or capture the IP addresses of every person visiting a particular website.

Under the vaguely written statute, it may even be able to capture the URL of every web page that you read, although the FBI refuses to confirm or deny whether it has done so.

Section 220: Nationwide Search Warrants for Electronic Evidence

Before PATRIOT, the FBI could execute a search warrant for electronic evidence only within the geographic jurisdiction of the court that issued the warrant - for example, the FBI couldn't get a New York court to issue a warrant for email messages stored by your ISP in California.

After PATRIOT, courts can issue warrants for electronic evidence -- your email messages, your voice mail messages and the electronic records detailing your web-surfing -- anywhere in the country.

Notably, Section 220 isn't reserved for terrorism-related investigations, despite the fact that PATRIOT was sold to the American public as a necessary anti-terrorism measure. **Instead, it applies in any kind of criminal investigation whatsoever.**

Section 220: Nationwide Search Warrants for Electronic Evidence

Section 220 allows the FBI to pick and choose which courts it can ask for a search warrant. This means it can "shop" for judges that have demonstrated a strong bias toward law enforcement with regard to search warrants, using only those judges least likely to say no -- even if the warrant doesn't satisfy the strict requirements of the Fourth Amendment to the Constitution.

By allowing courts to issue warrants to be served on communications providers in far-away states, Section 220 reduces the likelihood that your ISP or phone company will try to protect your privacy by challenging the warrant in court, even if the warrant is clearly unconstitutional.

A small San Francisco ISP served with such a warrant is unlikely to have the resources to appear before the New York court that issued it. Yet because you won't be notified if the FBI uses a warrant to get your electronic communications, your ISP is the only entity in a position to fight for your rights.

Section 223: Civil Liability for Unauthorized Disclosure

Section 223 made clear that the civil penalties that apply when investigators conduct wiretaps or seize electronic evidence without a court order also apply to unauthorized disclosure of communications that were legally obtained.

That means that even if investigators get a court order to collect your communications in the first place, they can't show them to anyone without court approval.

Section 223 also created new privacy protections by providing authority for agency heads to discipline federal officers who violate electronic surveillance laws.

This is the good news from Section 223

Unfortunately there is also some bad news with Section 223

Section 223: Civil Liability for Unauthorized Disclosure

Before PATRIOT, the US government could be sued under the same procedures and standards as anyone else who violated the Wiretap Act or the Electronic Communications Privacy Act (ECPA). Section 223, however, made it much harder for people to sue the government when federal agents violate these laws:

* You can no longer sue the government for "intentional" violations of the law, like you can sue everyone else. Instead, the violation has to be "willful," a much higher standard.

* Before, you could get a trial in front of a jury if you sued the government. Now, suits against the government are heard only by a judge.

* Unlike with any other defendant, if you want to sue the federal government for illegal wiretapping you have to first go through an administrative procedure with the agency that did the wiretapping.

That means, essentially, that you have to politely complain to the illegal wiretappers and tip them off to your legal strategy, and then wait for a while as they decide whether to do anything about it before you can sue them in court.

Section 223: Civil Liability for Unauthorized Disclosure

Before PATRIOT, in addition to being able to sue for money damages, you could sue for declaratory relief from a judge.

For example, an Internet service provider could ask the court to declare that a particular type of wiretapping that the government wants to do on its network is illegal.

One could also sue for an injunction from the court, ordering that any illegal wiretapping stop. PATRIOT section 223 significantly reduced a judge's ability to remedy unlawful surveillance, making it so you can only sue the government for money damages.

This means, for example, that no one could sue the government to stop an ongoing illegal wiretap. At best, one could sue for the government to pay damages while the illegal tap continued!

Overall Patriot Act Issues

- Lowers standards used for getting and using a wiretap. Legally the standards are much lower than previously.
- Increases the number of reasons that you can be surveilled or have your communications intercepted.
  - Terrorist Groups: Some controversy on designations.
  - Terrorist Acts: Providing Expert advice.
  - Non-terrorist Investigations: Many of the provisions, including some of the most invasive wiretap provisions, apply to any criminal investigation not just terrorism.

The standard defense of these kinds of laws is that "if you aren't doing anything wrong you have nothing to worry about".

This is fine as long as the government doesn't change its mind on what it considers "wrong".

Moreover, if you live near a designated individual you may now be under surveillance.

DMCA: Digital Millennium Copyright Act

What: Law created by Congress meant to stop copyright pirates from defeating anti-piracy protections added to copyrighted works, and to ban "black box" devices intended for that purpose.

Problem: In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright piracy. As a result, the DMCA has developed into a serious threat to several important public policy priorities.

DMCA Problem Examples

Limits on Fair Use: By banning all acts of circumvention, and all technologies and tools that can be used for circumvention, the law grants to copyright owners the power to unilaterally eliminate the public's fair use rights.
Already, the music industry has begun deploying "copy-protected CDs" that promise to curtail consumers' ability to make legitimate, personal copies of music they have purchased.

Consumers can be sued for fair use copying of CD's or DVD's or any other copy-protected material.

This includes making backup copies of CD's or DVD's or even in some cases making a mix tape.

Fair Use Issues

Perhaps more importantly, **no future fair uses will be developed.** After all, before the VCR, who could have imagined that fair use "time-shifting" of television would become common-place for the average consumer?

Copyright owners argue that these tools, in the hands of copyright infringers, can result in "Internet piracy." But the traditional answer for piracy under copyright law has been to seek out and prosecute the infringers, not to ban the tools that enable fair use.

After all, photocopiers, VCRs, and CD-R burners can also be misused, but no one would suggest that the public give them up simply because they might be used by others to break the law.

DMCA Problem Examples

Limits Competition and Innovation: Rather than focusing on pirates, many copyright owners have wielded the DMCA to hinder their legitimate competitors.

Example: Sony has invoked the DCMA to protect its monopoly on Playstation video game consoles, as well as their "regionalization" system limiting users in one country from playing games legitimately purchased in another.

Lexmark has used the DCMA to prevent companies from making and selling aftermarket laser printer toner because companies had reverse engineered Lexmark technology designed to prevent aftermarket toner sales.

DMCA Problem Examples

Limits on Research: In September 2000, a multi-industry group known as the Secure Digital Music Initiative (SDMI) issued a public challenge encouraging skilled technologists to try to defeat certain watermarking technologies intended to protect digital music.

A team of researchers at Princeton, Rice, and Xerox took up the challenge and succeeded in removing the watermarks.

When the team tried to present their results at an academic conference, however, SDMI representatives threatened the researchers with liability under the DMCA. The threat letter was also delivered to the researchers' employers and the conference organizers.

After extensive discussions with counsel, the researchers grudgingly withdrew their paper from the conference.

DMCA Problem Examples

Other potential problems in the future..

TIVO and other such services could be banned in the future.

Converting a store bought CD to MP3 on your computer could be illegal

Video recording a show and making a copy of it for archiving could be illegal if it contains a broadcast flag.

Broadcast Flags

What is it: The broadcast flag is a sequence of digital bits embedded in a television program that signals that the program must be protected from unauthorized redistribution. It does not distort the viewed picture in any way. Implementation of this broadcast flag will permit digital TV stations to obtain high value content and assure consumers a continued source of attractive, free, over-the-air programming without limiting the consumers ability to make personal copies.

This is the “official” MPAA definition

Basically, the broadcast flag is designed to prevent people from making copies of digital TV and Movies and putting them on the internet.

While this is already done, it is the threat of HDTV and other digital media that has the MPAA freaked out and scarred.

Broadcast Flags

Broadcast flags are not stopping at TV and Movies only. They are also being implemented into Digital radio.

Not Satellite radio, but digital radio that is received in your regular radio.

The idea is to prevent people from making copies of songs off the radio that are as good as CD's and passing them around without any money being made by the RIAA.

If these broadcast flags are passed and implemented, it could have a serious impact on your ability to record media and use it for yourself on different TV/Radio.

This issue has been around before with VCR's and bringing the movie industry to the ground. It didn't happen.

Technology and Civil Liberties

This section deals with how changes in technology, and specifically the law enforcement response to crime through technology, can impact civil liberties of individuals.

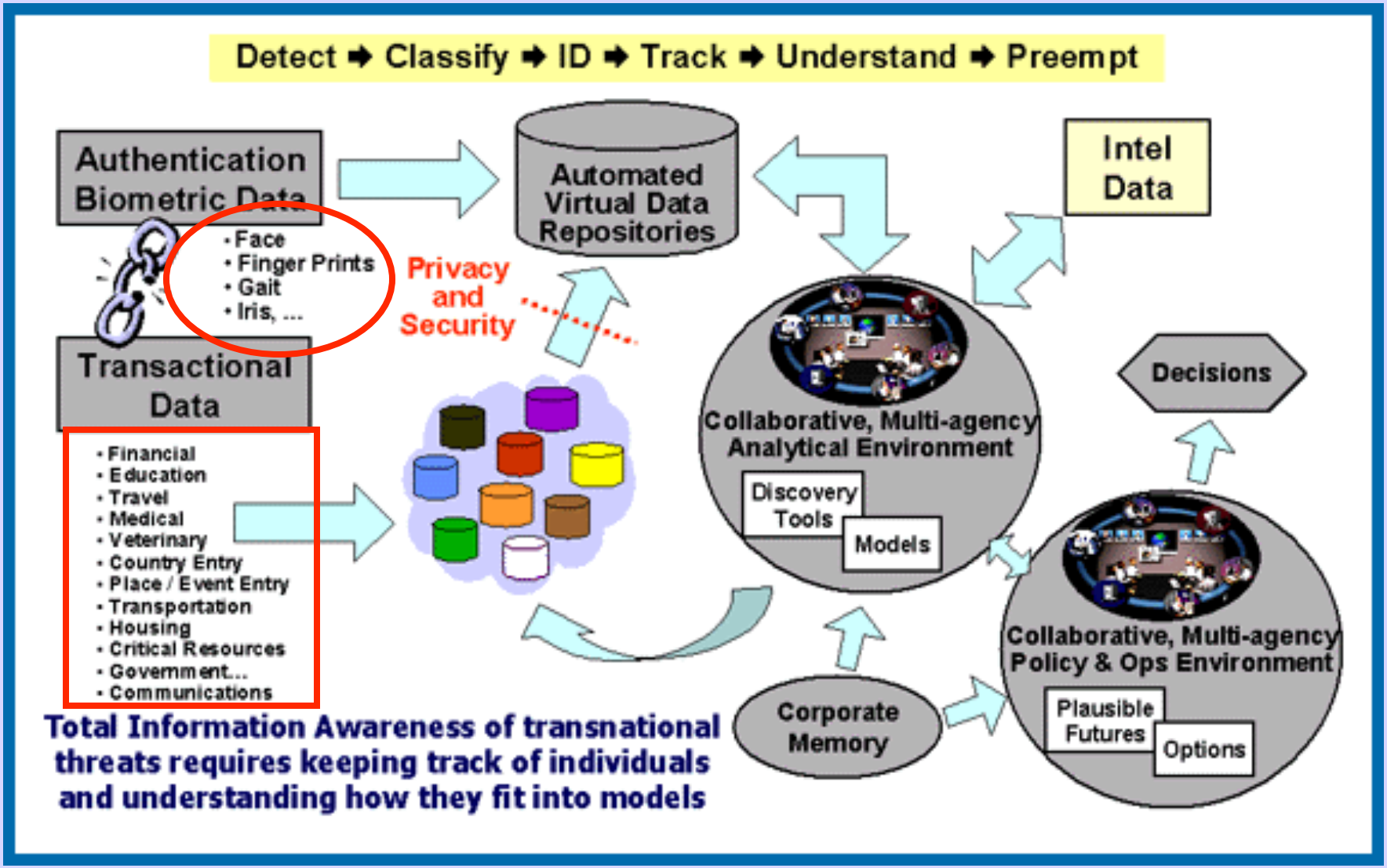
While there are several different areas in which technology impacts civil rights, we will deal with only a few.

1. TIA
2. Surveillance
3. Big Picture

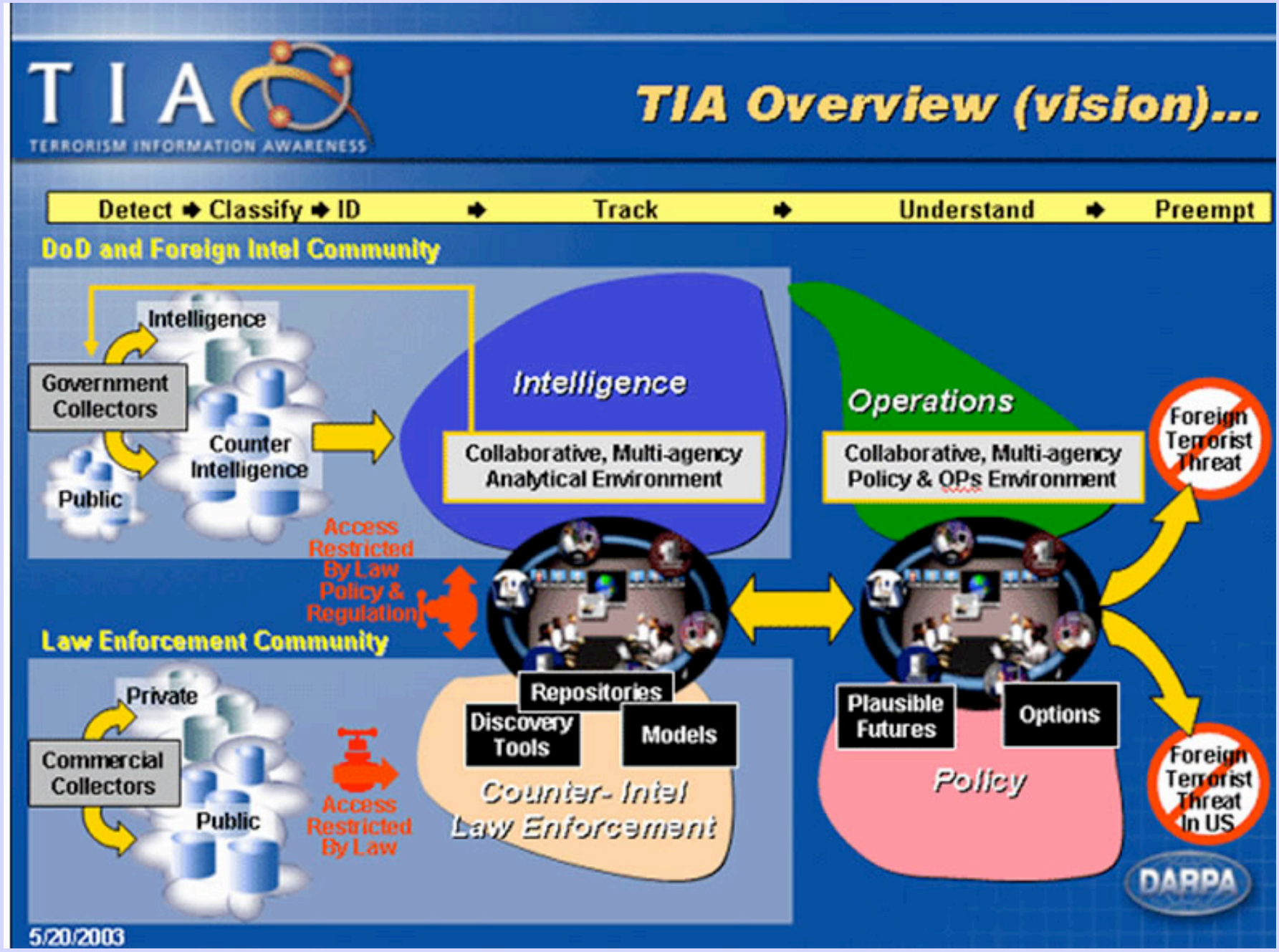
Total Information Awareness Program

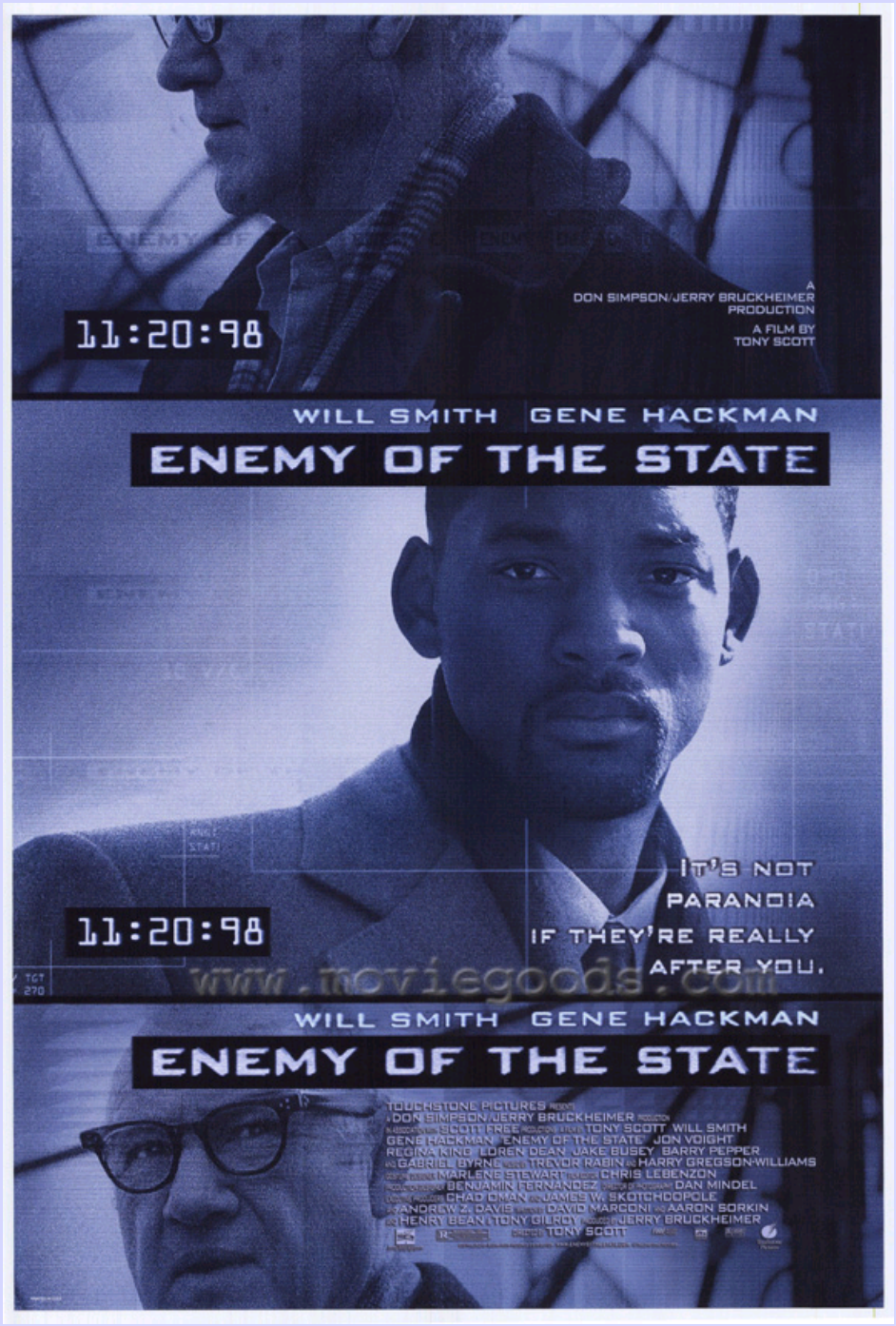
Knowledge is power

TIA Diagram

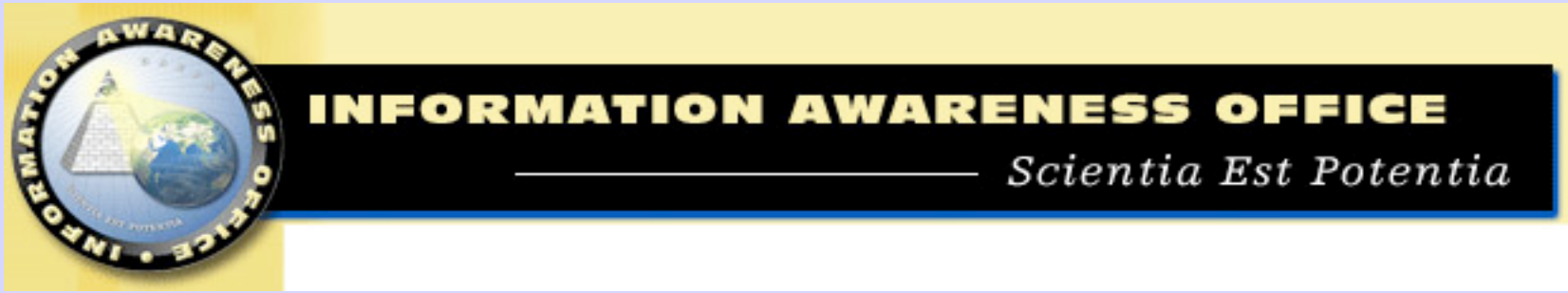


This is essentially high-tech profiling based on ALL of your supposedly private information.


TIA
TERRORISM INFORMATION AWARENESS
TIA Overview (vision)...
Detect ➡ Classify ➡ ID ➡ Track ➡ Understand ➡ Preempt
DoD and Foreign Intel Community
Intelligence
Government Collectors
Counter Intelligence
Public
Intelligence
Collaborative, Multi-agency Analytical Environment
Operations
Collaborative, Multi-agency Policy & OPs Environment
Foreign Terrorist Threat
Access Restricted By Law Policy & Regulation
Law Enforcement Community
Private
Commercial Collectors
Public
Access Restricted By Law
Repositories
Discovery Tools
Models
Counter- Intel Law Enforcement
Plausible Futures
Options
Policy
Foreign Terrorist Threat In US
DARPA
5/20/2003



This program sounds like something from Enemy of the State



"Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend — all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database."

William Safire, NY Times

"...it will provide intelligence analysts and law enforcement officials with instant access to information from Internet mail and calling records to credit card and banking transactions and travel documents, without a search warrant. Historically, military and intelligence agencies have not been permitted to spy on Americans without extraordinary legal authorization. But Admiral Poindexter, the former national security adviser in the Reagan administration, has argued that the government needs broad new powers to process, store and mine billions of minute details of electronic life in the United States. Admiral Poindexter, who has described the plan in public documents and speeches but declined to be interviewed, has said that the government needs to 'break down the stovepipes' that separate commercial and government databases, allowing teams of intelligence agency analysts to hunt for hidden patterns of activity with powerful computers."

John Markoff, MY Times

TIA Questions

Would the TIA program have prevented the terrorist attacks of September 11th?

NO, this database is designed to track only American citizens, not foreign nationals such as the terrorists.

THUS…

The question that needs to be asked is why is the government tracking us in this way?

What purpose does this information serve for them?

Death of the TIA

Funding for the TIA was killed in 2003, but many organization feel that it is to soon to determine if it is really killed.

More importantly, while the idea of the TIA is dead, as we will see many of the ideas within the TIA framework are still developing and functioning on there own.

At this point they are all independent, but in the future it will be easy and natural for them to be combined to give us a TIA functionality under a different name.

What kind of event will cause this unification?

Will it even take a single event to allow for the unification of data or will it simply be a bureaucratic response?

Surveillance Nation

Types of Surveillance

1. Cameras
2. RFID
3. GPS
4. Databases

Camera Surveillance

There has been a dramatic increase in the use of cameras and closed camera networks for use in Policing, crime prevention, and terrorism prevention.

- Superbowl in Tampa
- Chicago just implemented a 2,000 camera system.

The main idea is that cameras will help prevent things from happening in the first place and if they do happen they will dramatically improve investigations.

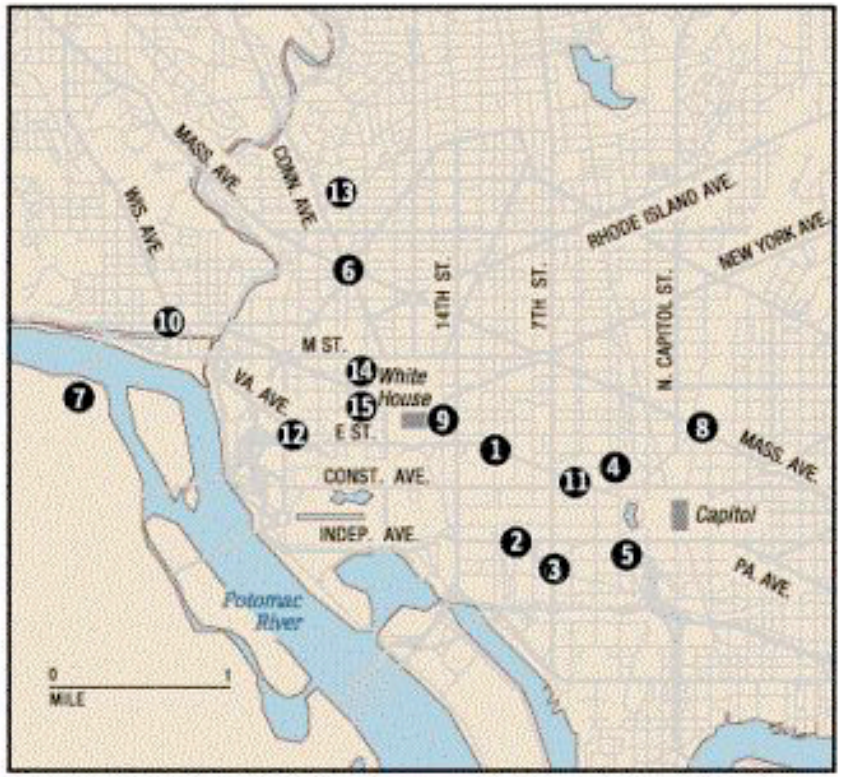
- Panopticon

In addition these camera networks have been supplemented with other advanced software systems to improve their effectiveness

- Facial Recognition
- Gait recognition

Map of the MPD surveillance cameras

The D.C. police department has 16 cameras at 15 sites that offer 360-degree views and magnify up to 17 times. Here are the locations of the cameras and their views:



[map adapted from a Washington Post diagram]

Source: D.C. Metropolitan Police Department

1. Old Post Office Pavilion [1100 Pennsylvania Ave. NW] Primarily for views of Penn. Ave. NW, from 14th St. to the Capitol.

2. Smithsonian Institution Castle [1000 Jefferson Dr. SW] Views of the entire Mall in both directions.

3. L'Enfant Plaza [480 L'Enfant Plaza SW] Views of southbound I-395, the Pentagon and Reagan National Airport.

4. U.S. Department of Labor [2nd St. & Constitution Ave. NW] Views of the Capitol, the intersection of Constitution and Penn. Aves. NW, and 3rd St.

5. Voice of America [3rd St. & Independence Ave. SW] Views of Independence Ave. from the Capitol to 14th St. and 3rd St. north to the Dept. of Labor.

6. Dupont Circle [1350 Connecticut Ave. NW] Views of Dupont Circle area.

7. Park Tower [1001 N. 19th St., Arlington] Views of Key Bridge, the Potomac River, the Kennedy Center and the D.C. shoreline along the Potomac.

8. Union Station [520 N. Capitol St. NW] Views of the plaza in front of the station.

9. Hotel Washington [15th St. & Pennsylvania Ave. NW] Views of 15th St. and Penn. Ave. NW between 12th St. and the White House.

10. Banana Republic [M St. & Wisconsin Ave. NW] Views of Wisconsin Ave. at M St. NW.

11. National Gallery of Art East Wing [3rd St. & Constitution Ave. NW] Camera installed only for special events at the request of the building management.

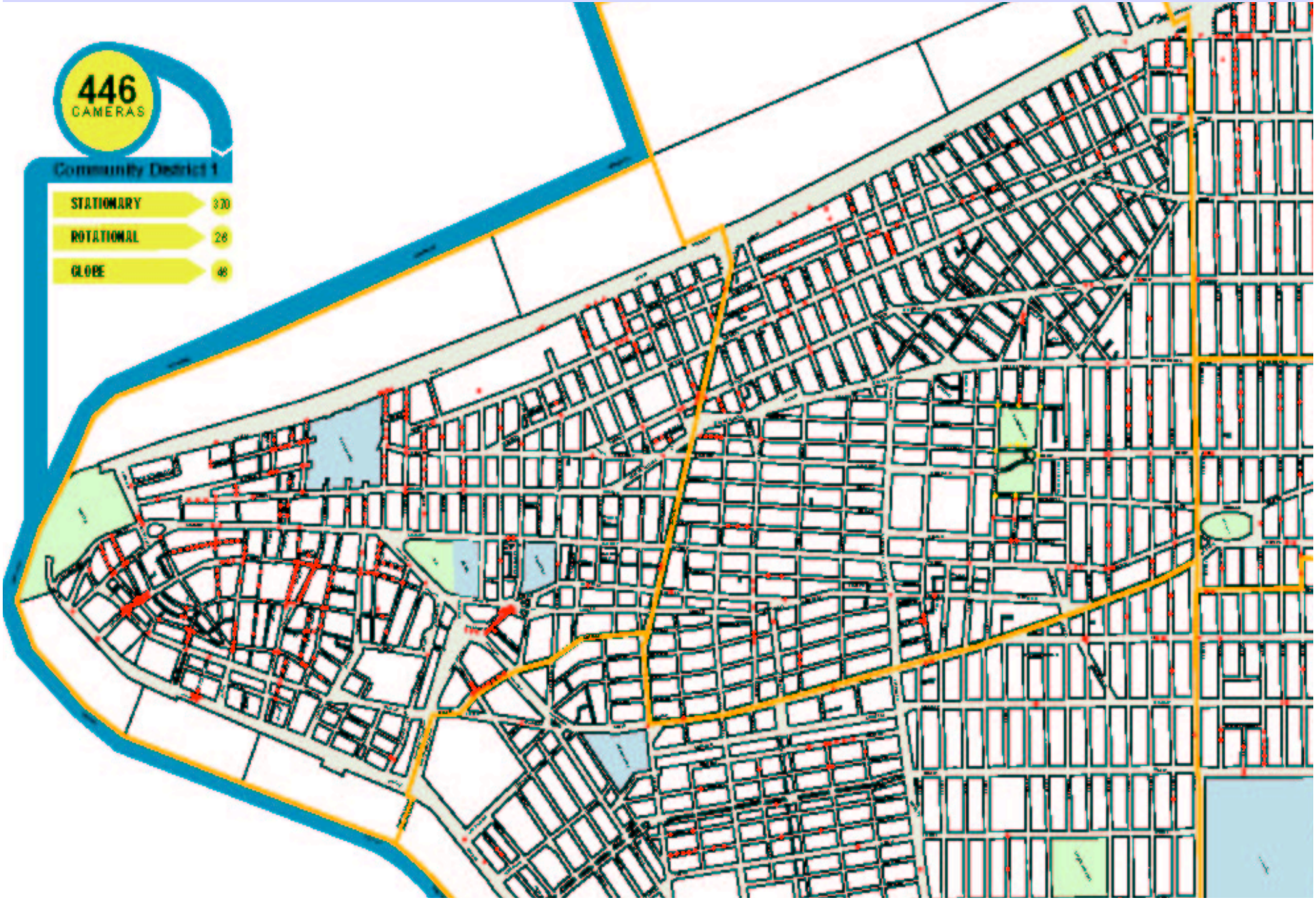
12. Columbia Plaza [24th St. & Virginia Ave. NW] Views of the Whitehurst Freeway, Roosevelt Bridge and Memorial Bridge.

13. Hilton Hotel [1919 Connecticut Ave. NW] Views of hotel surroundings and Conn. Ave. down to Dupont Circle.

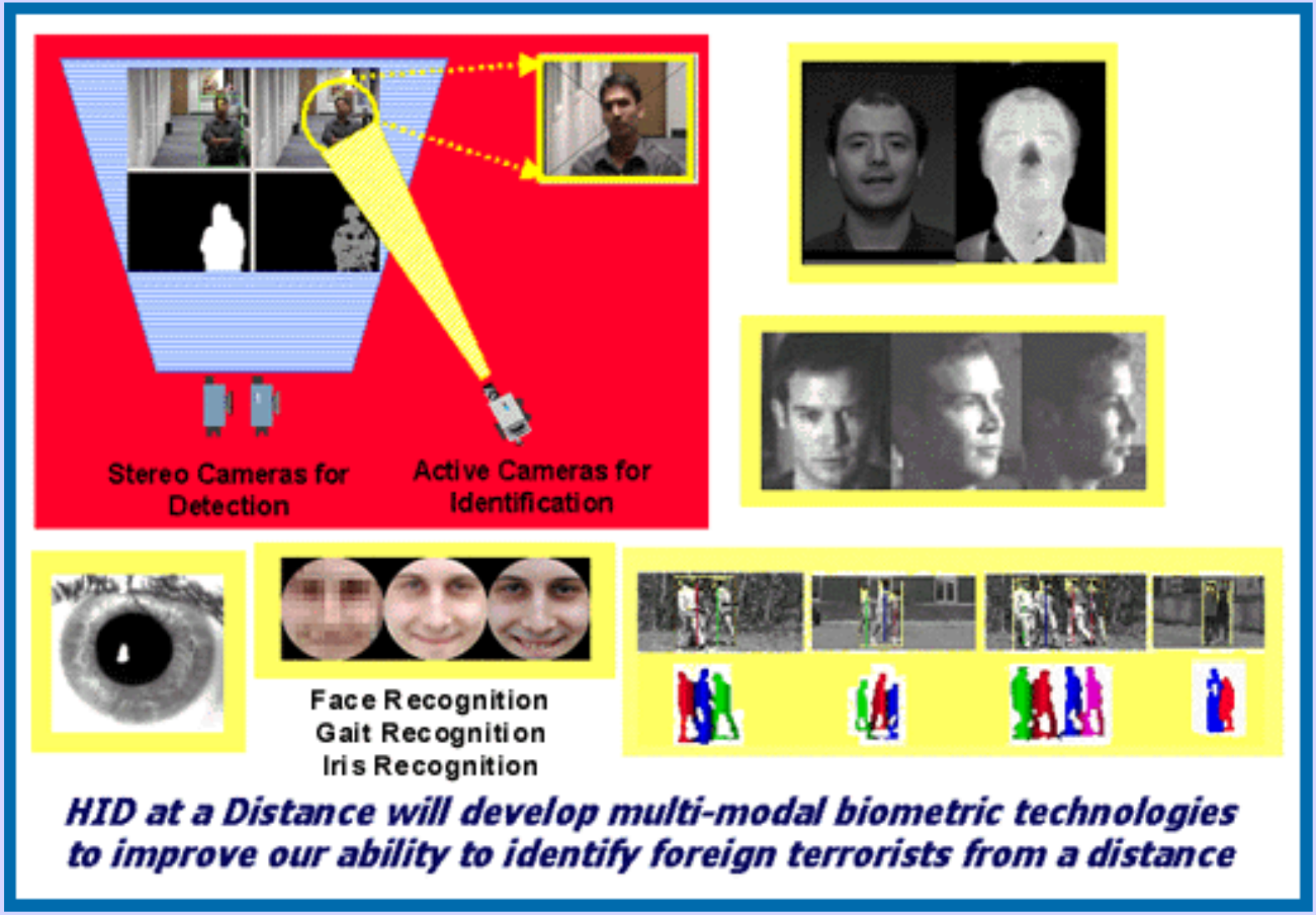
14. World Bank (I) [19th St. & Pennsylvania Ave. NW] Views of surroundings of World Bank buildings and Penn. Ave. between 22nd & 17th Streets.

15. World Bank (II) [18th St. & Pennsylvania Ave. NW] Views of surroundings of World Bank buildings and Penn. Ave. between 22nd St. and Old Executive Office Building (17th St.).

Map of Cameras in NYC



Facial Recognition and Gait Analysis



Used to conduct profiles, identify suspects, and add biometric data to already extensive databases.

Camera Surveillance

Potential Problems

1. **No Crime Reduction:** Research from Britain on the impact of cameras on crime has shown that street lights had more impact.

2. **Abuse:** Despite the fact that cameras have not been used in law enforcement for very long there are already numerous cases of abuse.

   In 1997, a top-ranking police official in Washington, DC was caught using police databases to gather information on patrons of a gay club. By looking up the license plate numbers of cars parked at the club and researching the backgrounds of the vehicles' owners, he tried to blackmail patrons who were married

3. **Social Impact:** When citizens are being watched by the authorities - or aware they might be watched at any time - they are more self-conscious and less free-wheeling

   knowing that you are being watched by armed government agents tends to put a damper on things. You don't want to offend them or otherwise call attention to yourself.

RFID Tags

Radio **F**requency **Id**entification

What: Small wireless devices that emit unique identifiers when hit with a radio wave from a RFID reader or sensor.

Most read only from short distances (less than 30 inches), although distance can be increased to almost a football field

Used heavily by private sector for security purposes, and increasingly being used by the government and corporations.

* Very Small

* Getting very cheap

* Readers are simple and cheap

Important aspect about RFID tags is that can contain data about an individual or product and that cryptographic protections are not as stable as many claim.

RFID Tags

* Consumer products of all kinds

  Wal-martification

* School districts and prisons

* Humans

* U.S. Passports

RFID Tags

Problems

1. **Passports**: As of right now the State department is not using ANY ENCRYPTION.

Thus, all personal information contained on the RFID (personal info. about the individual) could be read by any RFID reader.

2. **Danger**: Easy to "snarf" info. about citizens traveling abroad and put Americans in Danger of being targeted by Terrorists.

3. **Privacy**: As they become cheaper they will be included in almost every consumer product and will be easily read almost anywhere.

Profiling of people as they enter a store: what do they have on them

Tracking of people as they enter different stores

Data aggregation and sale of info by stores

where, when, how long did you shop and what did you buy

GPS

Global Positioning System: Series of satellites that are used to provide the exact position of a base unit.

Common in cars for use in navigation and increasingly being provided as an add-on feature for roadside assistance.

Onstar

Other Common and new Uses of GPS

1. **Navigation**: Cars, hiking, running.
2. **Cellphones**: Federally mandated to be in all cellphones (or a system as accurate) within a few years to provide for more accurate 911 responses.
3. **Prison/probationer Monitoring**: Monitoring of locations of probationers, parolees, and prisoners on workgangs.
4. **Children**: Wherify and other products that help parents monitor their childrens whereabouts.
5. **Surveillance**: Systems for parents to monitor their cars while kids are driving.
6. **Traffic Jam Monitoring**: In test phase currently.

GPS


TIMEX
SPEED+DISTANCE
GPS
TIMEX


CLICK FOR
PRODUCT
DEMO!


Power and
Service
Indicators
Five
Programmable
Buttons
Concierge
Service
Locate
on Demand

GPS

Potential problems

1. **Illegal Monitoring**: This has already been done in several criminal cases uses different methods.

New form of surveillance

Onstar cooperation/co-opting

GPS bug

2. **Crime Analysis**: Veritracks company claims to be able to "correlate" criminals who are monitored using GPS with crimes that have occurred to generate suspects.

3. **Abuses**: Illegal monitoring of individuals as a form of police deviance.

Monitor where people go and use it as blackmail.

Databases

As computers have become pervasive throughout the business world there are increasingly more and more databases containing information about people.

These numerous databases are increasingly being used for law enforcement purposes.

More importantly, these databases are also increasingly being used for less than legal purposes.

These numerous databases are also increasingly vulnerable to hacking and other cybercrimes, which can lead to problems of identity theft.

Databases

Types of Databases

Signature Capture: More and more retailers require customers to digitally sign for credit card purchases.

The manner in which these databases capture signatures can easily be used to create an exact forgery using, not very sophisticated means.

Biometrics: Databases that contain digital reproductions of physical characteristics, such as fingerprints, retina scans, and facial recognition.

These biometric databases are being increasingly used to increase security since 9/11.

Security of these databases is suspect in many cases. Leaving great potential for abuse.

Databases

Types of Databases

Other Information: Private companies gather this information about you for sale to merchandisers wishing to have more targeted sales information.

Information collected includes:

S.S. #, health information, salary, credit cards owned, marital status, automobile owned, mortgage amount, credit rating, etc..

Increasingly law enforcement agencies are linking to these databases in order to develop profiles, identify possible suspects and assist in investigations.

Databases

Problems with Databases

Database abuse: Michigan case in which several different officers used the databases to stalk women, find ex-spouses, and threaten motorists after altercations.

Crime: Criminals taping into these central databases that contain everything about people and using the information to commit crimes.

Identity theft

Fraud

Already this has happened with Choicepoint, the largest data aggregation company which sold records to criminals

Big Picture of Total Surveillance

While the TIA has been officially "killed" it still lives on in the continual growth and expansion of its component parts.

Data aggregation, GPS monitoring, RFID monitoring, Camera Surveillance, etc..

Although there is not one central repository for all of the data and it currently is not linked it is not a big step to link them all in the future.

Increasingly possible given the ever expanding CJIC and TIC into new growth areas

new companies, new fears, more profit, more control

What incident will cause the aggregation and unification of these disparate data streams?

Big Picture of Total Surveillance

Total Movement Surveillance of the future

GPS While driving

Cameras while driving and walking

RFID when shopping and entering locations

GPS/Cellular when talking and being anywhere

Financial, medical and other data monitoring

Biometric data when shopping, entering locations

Big Picture of Total Surveillance

In the future it will be easily possible to seamlessly track an individuals

* Movement (GPS, Phones, RFID, Cameras)
* Habits (RFID, Cameras, Databases)
* Purchases (databases, RFID)
* Health and Wealth (Databases)

In order to create:

* Profiles (criminal and consumer)
* Suspect lists
* Persons of interest


BIG BROTHER IS
WATCHING YOU