Lecture 9: Civil Liberty and Legal Issues in the War on Terror

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 voicemail 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 voicemail 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 voicemail 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 voicemail, 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.

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".

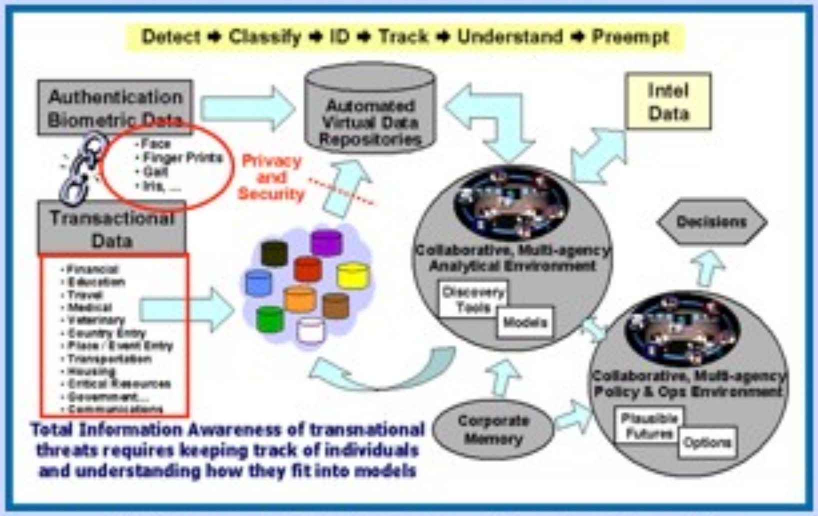
This is fine as long as the government doesn't change its mind on what it considers "wrong".

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

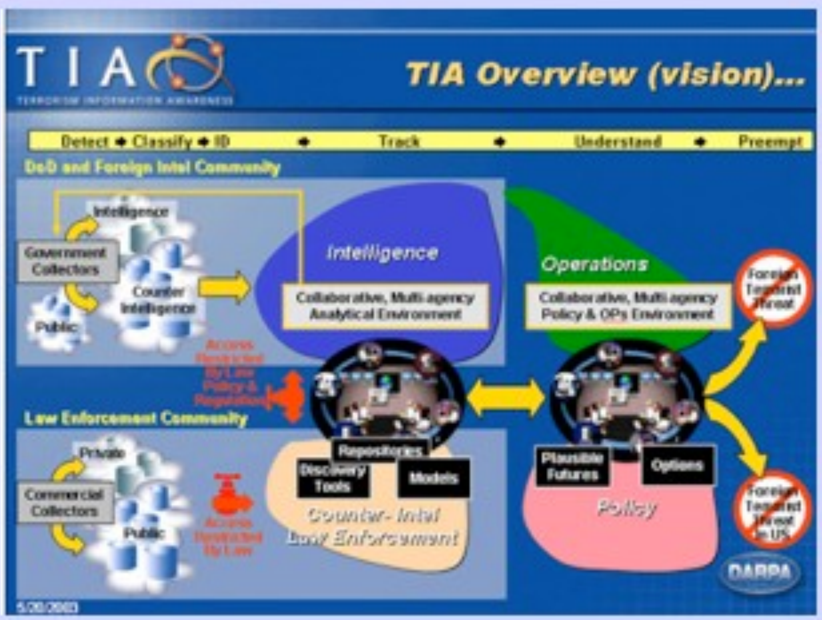
Total Information Awareness Program

Knowledge is power

TIA Diagram



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



This program sounds like something from Enemy of the State

INFORMATION AWARENESS OFFICE

Scientia Est Potentia

"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.

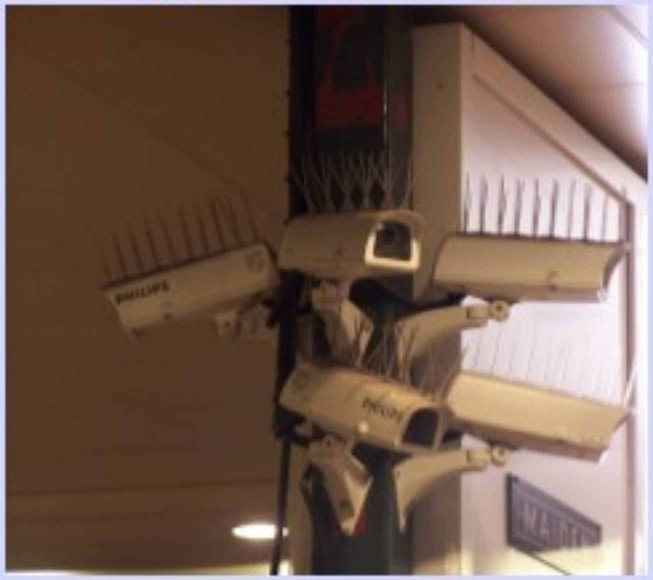
More importantly, while the idea of the TIA is dead, as we will see many of the ideas within the TIA framework are still developing and functioning on there own.

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]

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 [500 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.).

Source: D.C. Metropolitan Police Department

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.

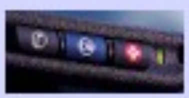
Common in cars for use in navigation and increasingly being provided as an add-on feature for roadside assistance.

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



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

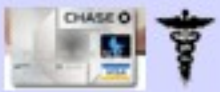
Total Movement Surveillance of the future

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

Assignment

- Find an article dealing with increased surveillance or tracking by Law Enforcement.
  - Can be a newspaper article
- Cell phone, GPS, Cameras, warrantless searches, etc..
- Write a compare/contrast article on the balance of improved security with loss of civil liberties and personal freedoms.
  - One page is NOT enough.
- Due Wednesday December 7th by 5:00 p.m.