**CERIAS Tech Report 2009-19**

# PRIVACY, SURVEILLANCE AND THE REAL ID ACT

by William Francis Eyre

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Graduate School ETD Form 9
(Revised 12/07)

# PURDUE UNIVERSITY
## GRADUATE SCHOOL
## Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By William Francis Eyre

Entitled Privacy, Surveillance and the Real ID Act

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

| | |
|---|---|
| Joshua Boyd Co-Chair<br>Chair | Victor Raskin Co-Chair |
| Aaron M. Hoffman | Christian Hempelmann |
| | |
| | |

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Joshua Boyd

Approved by: Mohan Dutta 13 February 2009
Head of the Graduate Program Date

Graduate School Form 20
(Revised 10/07)

# PURDUE UNIVERSITY
## GRADUATE SCHOOL

## Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:

Privacy, Surveillance and the Real ID Act

For the degree of Doctor of Philosophy

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Executive Memorandum No. C-22,* September 6, 1991, *Policy on Integrity in Research.**

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

William Francis Eyre
Signature of Candidate

2 March 2009
Date

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/c_22.html

# PRIVACY, SURVEILLANCE AND THE REAL ID ACT

A Dissertation

Submitted to the Faculty

of

Purdue University

by

William Francis Eyre

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

May 2009

Purdue University

West Lafayette, Indiana

To my son Richard William, my mom and dad, Carol Ann and William Arthur, and Sharon Hughes.

# ACKNOWLEDGEMENTS

The author would like to thank Sharon Hughes for her invaluable advice and guidance throughout the process, my parents for their help and support, my son for his understanding, and those who provided help and guidance. The author would like to thank the dissertation committee and the faculty and staff of CERIAS, especially Dr. Eugene Spafford. A special thanks to Dr. Christoff Hoffman. Also, thanks for help and support from my Culver classmates and fellow alums, Jim Hass, Mark Jones and Dan Gilbert.

TABLE OF CONTENTS

Page

# ABSTRACT

Eyre, William Francis. Ph.D., Purdue University, May, 2009. Privacy, Surveillance and the Real ID Act. Major Professors: Joshua Boyd and Victor Raskin.

American society in the present day is grappling with issues of privacy and surveillance. These issues, the technologies involved, and implications for the organization and function of American society are examined in this dissertation.

Public Law 109-13 contains the Real ID Act, and the implementation of this act has far-reaching ramifications for Americans' privacy. The Real ID Act, an exemplar of recent laws regarding privacy and surveillance, serves as a basis for discussing the development of a surveillance society and its potential harm to American citizens.

The dissertation begins by framing the evolution of the concept in American society, exploring anti-terror legislation as the latest assumption of extraordinary powers by the state in times of war and national emergency, and comparing previous abridgements of enumerated Constitutional rights in such times. It next discusses the implication of the Real ID as an insecure collection of databases, and then it examines the effect of Real ID on American citizens' privacy as a national identification card. States have resisted the implementation of the act on the bases that the act constitutes an unfunded mandate and damages privacy.

The new surveillance system erodes personal privacy and creates a threat to privacy and autonomy from both criminals and the government, or sometimes (due to insider abuse of data) both. The dissertation details the possibility of how

Real ID information access can be used against people in ways both legal and illegal, with comparisons to Great Britain; it also questions whether the government is even capable of handling increased information resources or whether such resources only provide more opportunities for improper access and misuse of personal data.

For most people, the developing surveillance state may only pose potential danger until someone is identified as a target, but its potential chilling effect threatens participatory democracy and the expression of legitimate political dissent. The goal of this dissertation is to increase awareness of the incremental erosion of privacy rights which, once surrendered, become increasingly difficult to regain. It also aims to question some of the security assumptions that justify this erosion.

# CHAPTER 1. SURVEILLANCE TODAY

## 1.1. A Day in the Life

It's an average day. Average Joe the Plumber and Jane Doe live in a high-rise condominium in Chicago and start the day by clicking on the morning news. Their television is fed using a cable box, TiVo or satellite connection to the High Definition Television (HDTV). Using the cable or satellite TV causes the television signal provider to know what channels they have on the TV at any time, down to the second, and allows the provider the ability to record in a computer log file those preferences. Additionally, if the individual has a DVR, the time and duration, as well as the content of the show being viewed, are also known to TiVo or whatever company administers the DVR software updates and management (Charny, 2004).

DVRs allow a two-way communication for the purpose of helping users select the next show they will like. For this goal to be achieved, the shows the users watch must be known to the preference prediction algorithm on a computer. This algorithm will help determine recommendations to the users based on that users' past viewing (This recommendation scheme rests on the assumption that the individual actually watches and enjoys the shows that appear on his/her screen.). The "recommendations for future viewing" feature is implemented using an algorithm which determines the genre and subject matter of shows the users appear to like (using a rational choice theory model in which it can be assumed that users will only view the shows they like and not select and view shows they do not like). The algorithm then fits the users' past selections to a set of preference scoring criteria, picking shows and/or movies matching those scoring

criteria and recommending the resultant list to the viewer. This is similar to the manner in which Amazon makes recommendations for books ("Million dollar Netflix," 2006).

This information has commercial value and is stored. It also has value in that it can give insight into individual interests. This could help content programmers, and whatever organization has the resources, understand the psychology of the viewer.

In a similar fashion, the HDTV itself uses a bi-directional data reception and transmission protocol (Svensson, 2008). This feature of HDTV was written into the specification to enable users to use video teleconferencing.

If Joe or Jane were to hook up their computer to the display, it could act as the monitor (screen) for the computer and the Does could perform all the functions they would normally perform in terms of computing using this display. They could also hook up their Webcam to this setup which would provide for greater definition when communicating with people at the other end of an Internet connection for a chat session. The corollary to this scenario involves the fact that everything displayed on the computer screen (the HDTV in this scenario) can be piped as data to the other end of an HDTV connection, in addition to the connection to the other end of the Internet connection; these would conceivably be two separate connections. These connections could be two dissimilar places, as the processor in the HDTV (the computer that converts HD digital signal to build the picture) has enough processing power to render the picture itself into a digital signal to send to wherever the TV is told to connect.

In the very near future, the Does will not need a Webcam for the recording and broadcast of the goings on in the field of view of their television. Apple holds a patent which describes a television screen with sensors interlaced amongst the

pixels which compose the display portion of the TV. These sensors will reconstruct the photonic input they receive to allow the TV itself to act as a camera. Additionally, using smaller or larger subsets of the sensors will allow the TV/camera to provide variable focal lengths, meaning that the TV can show close-ups and wide angle views with none of the traditional lens movement (or even a lens) associated with zooming in traditional models of picture capture (Fox, 2006).

One or both of the Does might then sign onto the Internet and check email. The visited Web addresses and emails are recorded in the ISP's database. Under the current United States Department of Homeland Security (DHS) Cyber-Initiative, established by classified presidential order, any communication that traverses a federal government network may be recorded by the National Security Agency (NSA) or DHS without the necessity of accessing the ISP's database (Nakashima, 2008). The reason for recording this information is in order that the United States is protected from terrorist cyber-attacks. All visits to government sites (i.e., IRS, CDC, DoJ, etc.) are recorded and NSA monitors and records all communications including Internet, voice and email (Bamford, 2008, p.179). AT&T also monitors the contents of Internet communications in real time (Singel, 2007).

Each click on an ad or link proffers a new piece of information for the ISP's database. The addresses of Web sites visited as well as the content of those sites are also, in the default configuration of the most used Web browsers, stored on the user's hard disk. The reason for this storage is that the browser can speed display of data (text and graphics) from the "cache." ("Deleting Web," 2006) It also leaves a permanent, barring user intervention, record of everything the user had "seen" (Once again certain assumptions are necessary; that the user did not click on a link which maliciously redirected a user to a site not described by the

link, and that those links which were clicked correctly offered sites and pages that the user viewed and enjoyed.).

In the Does' high rise condo's hallway there is a camera. So when they exit the door to the condo, their images are recorded by a camera in the hallway. At other times, when they have visitors, those individuals too are photographed entering and leaving. The elevator provides a camera image from the camera in the ceiling. As well the lobby and egress have surveillance cameras, or in the case of going into the parking garage, the elevator lobby and the exit are under surveillance.

Average Joe works in the suburbs and drives to work from the city. Jane works in the city's center ('the Loop' in Chicago's case) and takes mass transit.

Some transit systems have migrated away from paper tickets which can be paid for with cash to "Smart Cards" ("About smart cards," 2009). These cards require that processing occur based on the commuter's entry and exit points as well as the time those checkpoints were encountered. This processing is performed in order to automatically deduct the amount of the travel from an account. The account must be filled with money and this can be accomplished using a credit card. The ostensible purpose of the Smart Cards is to save money for the transit system and eliminate the fraud involved with people passing transfers to each other in order to get free rides (Godfrey, 2008).

Once the credit card is used for the purpose of payment, the transit card number and the credit card number are linked. Log entries must be made and kept of all transactions at each stage, and therefore all the data associated with an individual's transit system travels are known forever and can be mined or viewed any time thereafter ("Intelligent transportation," 2005, pp. 5-6). Data mining is the technique of using databases as input for algorithms that search for patterns and

identify characteristics and generators of patterns in which the data analysts' end users are interested.

In Joe's case, that of a commuter driving to work, the fact that he owns a car is registered with his state's motor vehicle bureau. This registration of the vehicle on its own can be considered a minor issue in terms of surveillance for the reason that vehicle registration has been required for many years. Massachusetts was the first state to issue registration tags in the United States in 1903 (Tortora, 1998) and this can be thought of as merely having been a tax which must be credited to the proper vehicle registrant. For surveillance purposes, the vehicle's plate number can be associated with an individual owner. If Joe stops for gas and pays with a credit card, the transaction is logged into multiple databases (O'Harrow, 1998, 2005).

There are now RFID readers along highways. The T.R.E.A.D. Act rules mandate RFID chips to be embedded in tires, and uniquely numbered RFID tags in individual tires to specific vehicles ("Intermec to support", 2002). The stated goal of the Act is to facilitate recall efforts in the case of recalls of defective tires by matching each tire to the vehicle and by extension, the owner. As Joe drives to work, he may encounter one or more of these RFID readers, and the time and location of the encounter can then be logged into a database (Warrior, McHenry, & McGee, 2003).

The other technology that can be used to track vehicles is the Tire Pressure Monitoring System (TPMS). TPMS is a technology that the National Highway Traffic Safety Administration has mandated will be implemented in all new passenger cars and trucks starting in 2007. The purported *raison d'etre* of the sensor is to detect whether tires are under-inflated (Kerr, 2007). The sensor transmits a unique ID number to the on-board system, mostly on one of two assigned radio frequencies, 315MHz or 433MHz. These signals can be picked up

at a distance with a directional antenna, and the initial ID number assignments are made by the auto manufacturer, so these are recorded in the database(s) in which all of the other part numbers associated with that car are recorded. Some sensors are embedded in the wheel assembly, and the tire must be removed to access them. These devices have batteries which last 7 to 10 years. Another option is to use a valve stem sensor, which behaves in a similar fashion (Kerr, 2007; “Spy my ride”, n.d.).

Concurrently, all cell phones now at a minimum have location assisting technology, and newer cell phones have assisted-GPS. The assisted-GPS cannot be turned off and will work even if the Subscriber Identity Module (SIM) card is taken out of the phone or switched with some other phone’s SIM card (K.C. Jones, 2007a). (The SIM card contains the numeric codes which identify the phone as one’s own for billing and service. The SIM card also contains a subset of the phone book data and text messages, including deleted text messages, associated with the phone. This information can be recovered forensically, so the system can even know exactly where the user was when having sent any given message ("Sim card," n.d.). Therefore, as Joe is driving along, because of the two way communication that defines a cell phone, his location is logged by the cell phone company, as often as every couple of seconds if the cell phone company sets up that phone’s tracking in that way. This type of location and tracking mechanism is ostensibly  in order that if Joe becomes lost or missing, the cell phone tracking records can be used to reconstruct his movements, and then to find him ("Missing persons," 2008, pp. 8, VI.A.14.).

Many new cars have on-board computers which record information. Some of this information regards the condition of the engine and various on-board systems. These on-board computers can also keep continuous records of the car’s speed at any given time. There are 30 data points that the federal government is going

to require of all electronic data recorder (EDR) equipped cars. The EDR will be a requirement for all new cars sold starting in the 2013 model year. As of 2008, many manufacturers have started equipping their cars with EDRs. In most cases the EDRs write over old information as new information comes in, the overwrite time being variable, but mainly engineered so that the 30 data points are available in the event of a crash, in that the insurance company and law enforcement can determine what the car was doing just prior to a crash.

In some cars, a vehicle status data recorder, which does not overwrite data and is always on, is included. The ostensible reason for installing this device is for manufacturers to determine if and when a driver violates the warranty, and what part (or parts) is (are) affected by the behavior which would void the warranty, such as racing (Gritzinger, 2008).

In addition, the onboard Global Positioning System (GPS) device communicates using a digital signal allowing the car's location to be precisely fixed at any given moment. This is a two-way communication which causes real time location information to be written to a database, and this information can be stored, or referenced through a tracking database. Various commercially available products facilitate the storage and retrieval of GPS-generated locational data, and they are used for various purposes. Police and intelligence agencies use GPS tracking on suspects' vehicles, with and without warrants (Hubbard, 2008). Likewise, car dealers who sell vehicles to customers who the dealer feels may one day need to have their car repossessed sometimes have GPS tracking devices on the vehicles and do not tell their customers about this "feature" (Vijayan, 2008). Some systems have components associated with the GPS that can be controlled from a PC. For instance, the person controlling the system, in addition to knowing where the car is at any time, could disable the starter ("GPS vehicle," 2008).

If there is a toll booth along the way to work, Joe will pass through the toll booth. Several tollway systems offer toll transponders which have the toll amounts automatically taken from an account which the driver charges with a credit card. Each transponder is uniquely numbered so that the correct amount can be debited for toll payment. The time and ID number of the transponder are written to a database for billing and to settle disputes. More recently the toll records have been used, not just for criminal investigations, but also in civil cases such as divorces, to prove the car was not where the lying spouse said it was at whatever time was in question (Newmarker, 2007).

The same toll lanes which offer this convenience also have cameras. The cameras photograph the vehicles that pass through the transponder lanes, and the reason given for having the cameras is to prevent fraud and misuse, and of course send tickets to those without transponders ("E-Z Pass," 2006). The fraud could consist of such instances as someone manufacturing a counterfeit toll transponder programmed with someone else's correctly guessed or deduced transponder ID number, or something as simple as the use of a stolen transponder (assuming the owner did not notice and report it, as when it would have been reported the toll passing capabilities would be shut off like a light at the central computer.). Also, in terms of fraud and abuse, people (not Joe, because he is a law-abiding citizen) might move the transponder between vehicles, switching the transponder between vehicles without registering and identifying the vehicle carrying the toll transponder to the tollway authority. Transponders can also be hacked, with the bad guy able to read another individual's legitimate transponder and then use the transponder code (Mills, 2008).

If Joe did not have a toll transponder he will, on the passage through toll booths in many cases, still have his travel recorded by a camera. Many toll booths used by people who pay with cash can also read the toll transponders. The cameras

are trained on cars traveling through in those lanes ostensibly to combat fraud and abuse and for crime prevention in general. These cameras can also be used in patrol cars.

The leading manufacturer of license plate readers (LPR) is Remington-Elsag, and the Mobile Plate Hunter 900 has cameras mounted on the squad car and connected to a database for checking the plates which the optical character recognition (OCR) software identifies. The system can read up to 900 plates per minute from up to 50 feet with 95 percent accuracy (Vlahos, 2008). Checking the plates once they are read is a trivial computer database lookup problem.

When Joe arrives at a garage in an urban area, the car is photographed on entering the garage, and he punches the button for a ticket which contains a magnetic stripe. When Joe exits the garage, if payment is made with a credit card, his identity is associated with the garage ticket (which contained the entry time and by inference a cross-reference to the pictorial record of entry) and the car's visit to and length of stay at the garage is written to a database. The stated reason given for this type of observation involves physical security (Haas & Giovis, 2008).

If Joe was to park on a city street in a downtown urban area and gets a ticket for staying in the space for longer than amount of time than for which he paid the parking meter, that information is entered into a database ("Parking ticket," 2008). There is a pervasive surveillance effect of parking patrol police department employees patrolling the streets with handheld computer-like wireless devices, but that was the old way. Today, the fact that many cities have instituted laws which require that cars which have more than a certain number of outstanding tickets logged against them are to be booted, i.e., fitted with the "Denver boot." The new way is that the parking patrol canvasses the streets using 26 vans, each equipped with LPRs and checking cars on both sides of the

street at 1,000 cars per hour. The license plates of the cars are compared to a list of wanted license plates (Washburn, 2007). The most efficient mechanism is for the license plate of the parked car to be transmitted to a central database and compared there. There is nothing to prevent the time, location of the query from being logged in the database, and many reasons to expect that the recording of the encounter will take place.

Many convenience stores, malls, commercial buildings and public thoroughfares now have digital video surveillance cameras trained on the pedestrians and patrons. The nine-inch black cube hanging behind the Starbucks team member's head is a security camera (O'Harrow, 2005). So when Joe goes in before work to buy a cup of Starbucks, his image is recorded, and presumably, if he pays cash, his preference can still be deduced using the record from the digital video camera.

If Joe or Jane were to withdraw cash from an Automated Teller Machine (ATM) on their morning break, the time and location, and picture from its camera is duly stored in a database ("Digital recording," 2004). The ostensible purpose of this type of surveillance is crime and fraud prevention and detection.

At lunchtime, Joe buys something for his wife with a credit card, maybe for her birthday, maybe a purse she admired. That credit card transaction, including a detailed list of items purchased, is recorded. After Joe returns to his workplace after lunch, and he swipes a card for access to restricted buildings and areas, that information is recorded in a database. There is likely a camera recording the transaction, and at any time in the future, that transaction's video can be accessed keyed on the financial transaction itself (Vlahos, 2008). There may be cameras in the lobby and/or trained on the building entrance at work. Those cameras will record his return to work. As of January, 2008, there were an estimated 30 million surveillance cameras in the United States recording the

goings on in public and publicly accessible commercial spaces. These cameras were recording 4 billion hours of images per week (Vlahos, 2008).

At work, Joe uses a computer to do his job. Many employers have installed monitoring software to ascertain what exactly Joe, and other employees like him, do on their computers. At the very least, the bandwidth providers know what he does on the Internet. Some corporations and government agencies employ key loggers, which record every key the computer user strikes. So when Joe sends his wife an e-card for her birthday, the boss will know. Of course many employees avoid doing any personal business on the computers at work for the reason that they are monitored. The reason given by employers for using key loggers and other monitoring software is to measure employee productivity and monitor activity, perhaps to prevent the theft of insider secrets or other nefarious actions on the part of the employee ("Internet and computer," n.d.). This type of surveillance, however, is passé, as employers can merely state in the employee handbook or anywhere they publish their policies that the employee has no reasonable expectation of privacy when using work related resources (Eureste, 2008).

Every phone call is logged to the telecom's databases, and recently, legal authority to conduct real-time wiretapping against wide swaths of the citizenry has been granted by the United States government to itself (Frederickson, 2008). This authority is in addition to the warrantless and illegal wiretapping which occurred (Bamford, 2008, pp. 210-211). The scope of the illegal surveillance and the amount of data siphoned off will never be known. The FISA Reform Act gave the telecoms retroactive immunity for their illegal actions in violation of the FISA law as it stood in the face of court rulings against the government. As Mark Klein, the AT&T whistleblower, who was never called to testify to a committee of Congress, whose lawyer's letters were never answered, said, "There will never be any hearings. It will die, and you'll never find out what they did" (Goodman &

Klein, 2008). The supposed reason for wiretapping Americans and making databases of the numbers they called and the numbers that called their numbers was that this type of invasion of privacy was necessary for anti-terrorism purposes. So Joe Doe makes a phone call to his accountant, and the phone number he calls is entered into the database, and quite possibly the content of his conversation. If he calls his attorney, thinking he has attorney-client privilege, but his attorney has represented a Muslim on a visa from Egypt in a personal injury case, Mr. Doe may well find that his attorney –client privilege has been waived (without him knowing that that is the case).

Joe Doe may call his banker, or broker, or travel agent, or his host at the casino. Because all of these individuals work at commercial entities which are classified as financial institutions under the terms of the PATRIOT Act II, his records, along with everyone else's who has dealt with these institutions, can be seized by the federal government without a warrant (Wolf, 2007), and he could easily be made the target of wiretapping (Risen & Lichtblau, 2005). No one will ever know if his conversations are listened in on, because eavesdropping targets are classified.

In large commercial buildings in urban areas, those entering must present a driver's license and sign a book in the lobby. There is nothing to prevent the names in those visitor logs from being entered into some type of database. Some would say the security types would be remiss if they did not record the information. The accepted reason for this type of tracking is for physically securing the building.

Most public and commercial spaces in large cities are under video surveillance. In urban areas, intersections in high-crime areas and intersections deemed to have a high rate of accidents are under video surveillance. Cameras are used to issue traffic citations by mail for violations of red lights (Washburn, 2007). The feeds are sent to centralized "command centers" where human operators may be

watching in real time. It is said that in heavily surveilled cities, such as Singapore or London, individuals' images in the city centers may be captured as often as 300 times per day (Murphy, 2007; Severance, 2007). The reason given for taking everyone's pictures all the time is to prevent crime, investigate crime, and provide for traffic safety. Currently, there are plans to install more video surveillance cameras in urban areas in the United States for anti-crime purposes ("Big bucks," 2008).

When Joe leaves, the surveillance regimen marches on: cameras recording his walk to the garage, the garage logging his exit, the toll transponder and camera logging his passage, the RFID readers silently reading his tires' RFID tags, the GPS and cell phone tracking systems marking his minute by minute progress, the computer in his car recording every acceleration, deceleration, stop and go. When he gets back to his high-rise in the city, more of the same – until finally the last thing he views before going to sleep, the least email he reads, the last Web page he views for that day, is recorded.

On the weekend, every book Joe checks out of a library is recorded, although sometimes the government has trouble collecting that information legally (Kronholz, 2003; Reutty, 2007). For every airline ticket purchased and rental car agreement entered into, the data is recorded. Every time Joe writes a paper check, this information is logged into databases, and if the check is to the wrong person or for too much money, the Federal Government is informed through a separate channel and program (*Bank secrecy act*, 2006).

Any time Jane signs up for a loyalty card (the cards which allow discounts on selected items when presented upon checking out), she is allowing a record of all of her purchased items to be stored in a database such that even if she pays cash for the purchases, every item purchased is associated with Jane ("Loyalty & stored," 2004). In many cases, the company issuing the card will want to learn the person's name and address, phone number, and age. The marketing reason

given by the merchant is to possibly mail sale papers to the loyalty card holder. This begs the question as to why the store needs all of this information, especially the individual's age, unless the question involves building a dossier (marketing profile) on the individual.

If Joe and Jane gamble at casinos, the loyalty cards, when used in machines in a casino, allow an exact record to be made and kept of all of their gambling activity, down to the exact second and penny of wager and payout and the exact time, down to the second, that the wager was placed. In some casinos, the machines are networked and this information is available in real time. The reason given by the casinos for this type of surveillance is so that if a person is losing, the casino can offer that person some type of perk, in order that Joe and Jane feel better about losing their money and will return more readily to play again (Binkley, 2004).

If the individual trades in the stock market, all of the transaction information is stored and the Security and Exchange Commission (SEC) knows what stocks people buy and when they buy those stocks. The ostensible purpose is to detect activity which would indicate insider trading activity (Countryman, 2003).
Many of these transactional data elements are stored with and include significant amounts of what could be considered ancillary information associated with each transaction. For instance, when storing information about a cash purchase at a store conducted using a loyalty card, the data elements might include or easily link to the individual's phone number or age, among other data items, which should not be strictly necessary for logging the transaction. The extra information makes correlation easier. Correlation is the key to linking databases together to get the maximum amount of information on each individual. Correlation is an important concept in data mining and data integration in surveillance applications. Correlation, in its most basic sense, is matching sets of data to each other based on common data elements in the data sets.

If Joe and Jane travel to an international destination, they are outside the sphere of American surveillance, and subject to the surveillance apparatus of the country to which they travel. Some countries, such as Britain and China, have as much or more in the way of a surveillance apparatus (Hope, 2008; Klein, 2008). Most countries have less.

In the case of recent voter purging incidents, non-correlations were claimed on the basis of as little as a single character being different between the subject's name as it was input and the name listed in the voter database (Goodman & Weiser, 2006). This is in contrast to integration in the surveillance realm in which correlation is desired. The purpose of correlation is to facilitate integration between elements of information in such a way as to easily connect information to an individual even in cases of incomplete or inaccurate informational elements.

Integration is the act of connecting data from various sources (Rao & Tripati, 2008). The data may have characteristics with varying degrees of similarity, and may mostly match up byte for byte. When the keys, or main identifying fields, such as names or SSNs, of the data are identical in each of the databases being integrated, the job of integration is easy. Most of the types of information available to a logically centralized database have various inconsistencies, misspellings, different forms of a name, similar names and different addresses for the same individual, etc. With information integration, when a misspelling is encountered, other information can be compared, allowing for an identity match or association of an informational element in a greater percentage of cases. The process by which this type of information matching is conducted involves resolution or reconciliation of the data (Bhattacharya & Getoor, 2007).

An example of integration might be the following: Joe is carrying Jane's cell phone because his cell phone broke. He might have to borrow a friend's (let's call him Jerry) car. So when Joe is driving along, the RFID readers send data

showing that it is Jerry driving along. But the cell phone tracking shows a match for Jane. But Joe parks in his regular parking garage and swipes into work with his ID. At this point, the integrated system can then correct the location tracking database to indicate the correct individual's movements (Joe's). The integrated system will also note that Jane is somewhere else because her transit card was used on the transit system, in accordance with her patterns, and Jerry's first car (he loaned Joe his second car) and Jerry's cell phone are seen moving along Jerry's normal route at the correct time. So even though the informational data points taken individually (cell phone, car) might have led to a mistake in tracking Joe, the integrated system can make the correct identification. This is the type of situation that becomes a selling point for VeriChip, the company that has gotten FDA approval for implants of RFID chips in humans. In cases in which the systems are working properly, 100% accuracy of identification of the correct human is possible (Greene, 2004).

In the late summer of 2008, the National Reconnaissance Office (NRO), which is responsible for conducting surveillance using earth-orbiting satellites, has started working with DHS to aim the satellites at American territory and American citizens. The program is known as the National Applications Office. Previously, privacy, national security considerations and other limits on the federal government's powers to conduct surveillance on American citizens prevented the use of military satellites to conduct surveillance of America and American citizens. The ostensible reason for the satellites looking down on America and Americans is to find weak points in security defenses and to conduct other anti-terrorism functions. A recently released GAO report noted that the program "lacks assurance that NAO operations will comply with applicable laws and privacy and civil liberties standards" (Gorman, 2008). The program is moving ahead nonetheless.

Beyond the details of tracking and surveillance of movement in public spaces, there are aspects to tracking and surveillance at a wider, integrated level. This integration involves commercially and publicly held data.

Acxiom is one company that aggregates and integrates all manner of public and transaction records. Aggregation is the procurement of large databases with information from one or more similar sources. The databases are then integrated with existent information in new, proprietary databases, or set up as standalone databases for easy access and searches, without being integrated per se. For example, collecting databases of property records, voter lists, driver's licenses, vehicle registrations, employment records, marriages, births of children, inheritances, lawsuits in which one has been engaged, everything on a credit record, credit card statements, schools attended and degrees held, and then combining these databases, or making the links between them seamless, fast and easy to search for information on an individual, represents aggregating information and then integrating it. This is what Acxiom does, and this information is combined into dossiers of individuals' lives that are available to anyone to buy for $50 (Behar, 2004).

Privacy advocates in the late 1990s had been alarmed at the amount and type of information that commercial and government entities were amassing on individuals. These privacy advocates were concerned that the manner in which and amount of information collected represented what was tantamount to an invasion of privacy. At the time there were calls for discussions on the appropriate manner in which to place limits on this informational aggregation and integration. However, the terrorist threat and the events of 9/11/2001 changed the context of the discussion and the discussion of privacy took a back seat to a discussion of the virtues of surveillance in The United States in contemporary American society.

Individuals are subject to surveillance and tracking technologies for various reasons with varying goals. These reasons may be partially constructed with commercial components, have national security implications and/or engage law enforcement goals and are central to the rationale for collection and storage of tracking and surveillance data. The goals would follow from the rationale; more profit in the case of commercial considerations, and security and continuity of operations in the national security and law enforcement scenarios. The ostensible reason of protecting the citizens is given as a reason for tracking and conducting surveillance against all citizens. Central to the question regarding the use and abuse of surveillance and tracking methods and technologies is the concept of privacy.

As illustrated with the Does, a person might go through the day and have her movements and activities tracked with the aid of a variety of technologies which provide convenience but sacrifice privacy. The simple use of common devices and everyday conveniences makes almost all of the Does' actions and movements traceable--probably without their knowledge or consent. In many cases, tracking and surveillance data are produced as second order effects, by-products of the primary purposes of the technologies. In cases in which tracking is the central tenet of the technology, these technologies have as their primary selling point the safety of the individual. This is the case with the need to locate the source of 911 calls from cell phones, or the use of satellite tracking of vehicles in cases in which drivers go missing. The tracking component is sold to the consumer and in a philosophical sense to the public, under the pretense of making rescue efforts easier as well as easing the enforcement and prosecutorial efforts of law enforcement and the criminal justice system.

A vast amount of data is available about any given person, and it takes only being labeled as a suspect or target for all of that data to be accessed. The

questions of privacy and surveillance therefore revolve around the question of access to the data, by whom, and for what purpose.

This dissertation will discuss the potential loss of privacy the average American citizen faces in daily life and the danger to American citizens' privacy that the implementation of the Real ID Act represents. It will be argued that this danger far outweighs any increase in security that Real ID would provide.

Supporters of the Real ID contend that it is the proper way to implement the type of secure ID that the 9/11 Commission recommended. Detractors are concerned that the implementation is insecure, that the costs are too high, that it represents an unfunded mandate to the states, that it represents a national ID card which Americans have resisted every time that suggestion was floated and that it will be used for more purposes than it was originally intended.

The frame in which these arguments will be presented consists of several elements of civil society that will impact or be impacted by the adoption and use of a Real ID. The first is the American concept of privacy and the manner in which this "right" was constructed from interpretations of the Bill of Rights in various Supreme Court decisions as well as societal norms and statutes addressing privacy. Aspects of privacy to be discussed include the expectation of privacy in communication, speech and association. The literature regarding pre-9/11 and post-9/11 thinking about privacy is explored.

The government's reaction to the terrorist attacks of 9/11 has changed the focus of the privacy debate through the granting of extraordinary powers to the government to fight terrorism. The history and effect of various laws enacted during times of war and national emergency will be surveyed. Restrictions of liberties such as the suspension of habeas corpus and the restriction of speech and assembly will be discussed in a historical context. The restrictions on

liberties in the past will then be compared with the restrictions on liberties that the PATRIOT Act and various government surveillance programs represent.

The discussion then turns to terror, terrorists and terrorism and the role these play in the movement of society away from the idea of the fundamental liberty of the individual. It questions the idea that the safety of the state depends on individuals giving up their constitutional rights.

Assumptions regarding surveillance and the role surveillance plays in the prevention of terrorism will be discussed, as well as some of the effects of the surveillance state on the individuals living under a surveillance regime.

The dissertation examines the Real ID Act and its implementation according to the current rules enumerated by DHS, and it examines the role Real ID plays in making the country safe from terrorism. Simultaneously, it will discuss the privacy-destroying and surveillance aspects of the use of the Real ID. The role of databases in the Real ID implementation will be examined, as will as potential abuses of information by enemies and others. In this way, the reader can start to form an informed opinion as to whether the Real ID Act will or will not make American civil society safer and if the costs associated with a supposed new level of safety or (in)security are acceptable.

## 1.2. Privacy

What is privacy and how is it a right? Most individuals have an intuitive sense of what the construct of privacy contains. In Constitutional terms, privacy is not an enumerated right, yet it is something that individuals in contemporary American society have come to expect. The effect that technology has had on privacy and people's expectations of privacy is also germane to the current societal consideration of the concept of privacy. Societal norms regarding privacy are

important to consider, as the evolution of privacy as a right, and some would say, as a civil right (Radil, 1999), has progressed. The concept of privacy as a right in American society has developed historically throughout the years the Republic has been in existence as a logical extension of enumerated Constitutional rights. What does it consist of?

Justice Brandeis famously said that privacy “is the right to be left alone” (Warren & Brandeis, 1890). Some contend that privacy has to do with having some measure of anonymity when one goes out in public (Slobogin, 2007). Others might contend that it is the ability to keep information about various aspects of one’s life private to various groups of people with which the individual chooses to share the information. The latter contention goes to the theory of controlling the dissemination of one’s private information (Froomkin, 2000).

Based on their sense that individuals and institutions in power will seek to expand that power, the Founders ratified the first ten Amendments to the Constitution as the Bill of Rights (McWhirter & Bible, 1992). The Bill of Rights took effect in December of 1791. Among the rights enumerated in the Bill of Rights are such guarantees as the First Amendment freedom of speech, First Amendment freedom of association and assembly, Fourth Amendment freedom from unreasonable searches and seizures, Fifth Amendment rights against self-incrimination, Sixth Amendment rights to trial by jury and the right to a speedy trial and the Eighth Amendment prohibition against cruel and unusual punishment ("Bill of Rights," 1791).

These rights were grounded in the enlightened philosophies of the great European thinkers of the day and represented a breakthrough in the establishment and protection of the rights of individuals against “bad” governments. Forms of bad governments in the European tradition generally took the form of feudal and despotic governments, although the shadow of theocracy

in the form of the Catholic Church and Puritanism overlay much of the theory of governance of the time (McWhirter & Bible, 1992).

Court decisions have shaped the discussion of privacy in the United States over the years. An early discussion in a law journal regarding privacy came in the form of a situation described by Warren and Brandeis regarding the making and use of an image of an individual in the public space (Warren & Brandeis, 1890). Foreshadowing the invasion of privacy by the zealotry of today's paparazzi, the authors decried the gossip-mongering of their time thus, "The press is overstepping in every direction the obvious bounds of propriety and decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade…" (Warren & Brandeis, 1890, p. 196). The authors concluded that if individuals felt their privacy had been invaded, their remedy would be in the civil courts.

One of the first modern decisions regarding privacy came in the form of *Griswold v Connecticut* (1965) (McWhirter & Bible, 1992, p. 96), which had to do with the rights of individuals to practice birth control in the privacy of their own homes. "In *Griswold* five justices were willing to find a constitutional right to privacy, two in the 'penumbras' of the Bill of Rights, three in the Ninth Amendment… With this decision the right to privacy had finally found its way into the constitution" (McWhirter & Bible, 1992, pp. 98-99).

It is this lesser-quoted or used Ninth Amendment of the original ten amendments that are the Bill of Rights, which specifies: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people" ("Bill of Rights," 1791). The Ninth Amendment forms the basis for Supreme Court decisions which formalized the right to privacy. Justice Goldberg determined that to not enforce the "unenumerated" rights that the Constitution specified would "disparage" those rights (Tushnet, 2008, p. 182).

In *Paul v Davis (1976)*, an individual who had been arrested but not convicted found his name and face on a flyer distributed by the police to shopkeepers in Louisville, Kentucky, with others labeled as known shoplifters. After the charges against him had been dropped, he sued the police for invasion of privacy. Ethically, the police were in the wrong on many counts, especially in the principle of a man being innocent until proven guilty, yet Judge Rehnquist ruled against the individual because Mr. Paul had brought suit under the wrong theory of law; he should have sued for defamation (Parent, 1983, p. 304). Thus, the law takes a narrow view of the definition of privacy and it is not necessarily in line with an intuitive understanding of privacy.

The concept of a “reasonable expectation of privacy” is a well developed concept in discussions of law. This “reasonable expectation” concept is used in relation to discussion of what information can be gathered and used in court by law enforcement, employers, and other actors with power over the individual based upon what the individual says or does where and under what circumstances the speech or action occurs, and who can appropriately discover the speech or action. This concept of “reasonable expectation of privacy” was introduced as a Fourth Amendment protection in *Katz v. United States* in 1967 (389 U.S. 347). The case involved the contention of the government that since a pay phone was public, bugging the phone booth without a warrant did not impinge on Fourth Amendment protections (Slobogin, 2007, p. 12). The Court ruled that the Fourth Amendment protected people, not places, and that if society considered it “reasonable” that an individual was in a place and acted in a way that assumed that their actions or discussions were private, Fourth Amendment protection was implied. The Court drew the line at openly public behavior, so that any discussion in a restaurant or on a public street would not assume the guarantees of the Fourth Amendment.

The question became one of what information is appropriate for various parties to know and use and how the information should be used. The general tenor of this concept has to do with what information can be legally used against an individual in a court of law.

In instances which would involve the Fourth Amendment, in the past there had to have been a probable cause finding that a crime probably had been, probably was being, or probably was about to be committed to eavesdrop or conduct other surveillance. That concept of law, however, is now considered pre-9/11 in its thinking and application. The PATRIOT Act and subsequent additions and expansions would change all of that (Abele, 2005). The PATRIOT Act and the accompanying Acts, as well as the guidelines under which the FBI operates, require no finding of that nature in order for the government to conduct surveillance against American citizens. The most recent FBI guidelines reported in the mainstream media indicate, according to Caroline Frederickson, director of the ACLU's Washington legislative office, "…the FBI will be give carte blanche to begin surveillance without factual evidence… These guidelines will lead to political witch hunts and more unwarranted investigations of political enemies and peace groups." The FBI will be allowed to employ techniques from the period that led up to the Church Committee hearings, e.g., recruiting of informants, infiltration, disguise, etc. (Johnson, 2008)

The common misconception in contemporary American society is the saw that surveillance advocates trot out in which the desire for privacy is equated with a desire to hide some type of criminal or deceitful information or act. This is the "nothing to hide" argument for surveillance. This "nothing to hide" argument has been described as the "most common retort against privacy advocates" (Schneier, 2006). Yet there are many instances in which criminal deceit is not reason for a person's desire for privacy, but rather an individual choice.

Throughout the history of the Republic, there has been an acknowledgement and codification of the fact that privacy exists as a right and there are classes of instances of violations of that right to which the injured parties can seek remedies through the courts. In 1905, the Georgia Supreme Court in *Pavesich v. New England Life Insurance Co.* concluded that a "right of privacy in matters purely private is…derived from natural law" (Solove, 2006, p.13).

These dimensions, of information availability and dissemination about an individual, as well as direct observation and eavesdropping of an individual, describe and frame the concept of individuals' privacy. These dimensions have to do with aspects of individuals' lives that may not be criminal, but may involve information that the individual does not wish to have commonly known. Whether or not a person has cancer, or a taste for some food that may not be popular in the culture or locale (think of a vegetarian, cast into small town life in cattle country in Wyoming), or any one of a number of informational items, that may not necessarily be criminal, the individual may still prefer for whatever reason to keep it private. It was a matter of natural right that was codified into law, in which eavesdropping was a violation of common law even in Colonial times, with eavesdropping defined by William Blackstone in 1769 as "…listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse…" (Solove, 2006, p. 4).

In the years leading up to the events of 9/11/2001, the literature indicates that the progression of privacy rights of individuals was in the direction of greater individual rights, choice and privacy. With the advent of computers and the ability to collect, store and aggregate large amounts of data, even pre-9/11, privacy rights were being marginalized in the quest for data useful to marketers. Privacy was eroded by the ability of actors with computers and databases to share information easily. Communication and tracking technologies have served to

erode individuals' privacy. The erosion has occurred due to the ascendance of perspectives driven by commercial and law enforcement considerations.

A review of the literature showed that there are no neat boundaries which can be drawn around the issues surrounding individuals' privacy and privacy rights as these issues touch on every aspect of an individual's life, at all points every day. This observation is illustrated by the case of the Does in the opening just going to work in the morning. Some aspects of privacy engage First Amendment rights, some, the Fourth Amendment.

Some of these privacy rights (association and speech and search and seizure) are life and death issues under the PATRIOT Act, subsequent acts, and executive orders. The original PATRIOT Act, which has been greatly expanded with the passage of subsequent laws, allows the designation of groups as terrorist organizations, even though these may have been peaceful protest groups which an individual might have thought were protected by the Constitution and therefore which they were free to associate. This state of affairs started with selective and politically expedient use of the designation "terrorist organization" by the State Department under the 1996 Antiterrorism Act (Cole & Dempsey, 2002, p. 137).

Closer to home, the threshold for the declaring something to be "domestic terrorism" is the commission of "acts dangerous to human life that are a violation of criminal laws…[and] that appear to be intended…to influence the policy of government by intimidation or coercion." This part of the Act, written in a Minnesota state law mimicking the Act, allowed protesters who were planning actions of civil disobedience, in the spirit of the 1960s protests, to be arrested and charged with conspiracy to riot in the furtherance of terrorism in Minneapolis/St. Paul for the Republican National Convention in 2008. In this

case, the citizen “terrorists” were arrested and charged preemptively, before anyone had protested anything (Goodman, 2008).

Even if an organization is not declared to be a “terrorist organization” but found under Section 411 by the Secretary of State to “undermine U.S. efforts to reduce or eliminate terrorist activities,” and was shuttered under the provisions of the PATRIOT or subsequent Acts, an individual who contributed money to the group could have his or her assets seized. Thus, under the existing laws, protesting the passage of legislation extending and expanding the USA PATRIOT Act could result in an individual’s assets being forfeited due to the individual contributing money to a protest organization considered by the Secretary of State to be an organization which undermines U.S. efforts to reduce or eliminate terrorist activities. Some might argue that this circumstance represents a circumvention of the American political process (Abele, 2005, p. 30).

Illustrative of the concept of privacy is the question of Internet and email communications. Communication as a First Amendment right and the surveillance of protected political speech is one facet of the privacy question. The literature explored for the purposes of this discussion examines the legal community’s stance on the question of privacy regarding email communications, Web searching and surfing, and physical tracking.

The most salient Constitutional question of privacy and the Real ID Act has to do with another enumerated First Amendment right, freedom of assembly. Freedom of movement is implicated directly in the concept of freedom of assembly. If one is under surveillance at all times, with all movements known and catalogued, is there a freedom to assemble? Generally, one can consider that freedom of assembly and freedom of speech are married, as they are in the First Amendment to the Constitution. If one right is abridged, the other is also abridged. What good would it do for individuals to meet but not be able to speak

freely? And conversely, what purpose would it serve to be able to speak, but not to be in personal contact with those one speaks with? A corollary is that due to the manner in which phone calls, emails, and all financial transactions are logged, if one's movements are tracked, there is not even the ability to donate to an organization such as the American Civil Liberties Union (ACLU) without the government knowing. The ACLU is, at the time of this writing, a legitimate, non-terrorist political organization. The ACLU is an impediment to the implementation of some conservative policies of the government, however, and therefore may at some point have its membership and donor lists come under greater scrutiny.

The issue of anonymous association was addressed but not resolved in a 1972 case, *Laird v. Tatum* (408 U.S. 1). The United States Army infiltrated and conducted domestic surveillance against groups that were planning demonstrations and peacefully airing their grievances. The Court did not address the question of privacy in one's associations. Instead, deciding that the plaintiffs had not shown that they were damaged, the Court decided that the victims of the surveillance had no standing to challenge the constitutionality of the surveillance and the Court refused to issue an injunction against the Army to stop domestic spying. Chief Justice Warren E. Burger, writing for the majority, ruled that "the 'subjective chill' that could result from fear that information collected by the government might someday be used to harm those about whom the information had been collected was not a sufficient justification to issue an injunction…" (Kuhn, 2007, p.74). However, in the dissent in 1972, Justice William O. Douglas argued that there should not be a need to show harm in order that the Court would be able to review the Army's surveillance program:

> The Bill of Rights was designed to keep agents of government and official eavesdroppers away from assemblies of people. The aim was to allow men to be free and independent and assert their rights against government. There can be no influence more paralyzing of that objective than Army surveillance. When an intelligence officer looks over every nonconformist's shoulder in the library, or walks invisibly by his side in a picket line, or infiltrates his club, the America once extolled as the voice of liberty heard around the world no longer is cast in the which Jefferson and Madison designed, but more in the Russian image. (Kuhn, 2007, p.74)

Under scholarly definitions of terrorism, the terrorists commit terrorism in order to influence target populations. When the terrorists succeed in effecting changes, the terrorists are said to have been successful. Possibly to the detriment of American civil society, it would seem that in reaction to terrorists' attacks, changes have been made to the United States' government's recognition of the rights of American citizens, with freedom and privacy having been eroded.

An example of thoughts about privacy in the literature regarding First Amendment issues in the age of the Internet, the Internet Age having started before the terror attacks of 9/11, would help to frame the question of the normative privacy considerations American citizens, as members of a society governed under the laws consonant with the United States Constitution, had come to expect. The pre-9/11 literature on the subject demonstrates a stark contrast with the post-9/11 literature, and the anti-terror considerations which caused Americans and the Congress as the citizens' representatives to abandon privacy rights will be explored.

### 1.3. Privacy in Internet Communications – The Literature

That privacy considerations involving Internet communication are seen as a moving target is a theme throughout the literature. This is due to the fact that the Internet and the technologies associated with and used in conjunction with it are evolving rapidly (Brownlee & Claffy, 2004; Grier, 2006).

In the main, Americans have had a different attitude throughout the early history of the Republic than Europeans regarding privacy. Americans showed a preference for a greater degree of property rights-based physical privacy. This is evidenced by a history which includes the development of privacy enhancing technologies (a phrase also used to describe technologies to help individuals maintain privacy in discussions regarding computer-related privacy issues).

Among these privacy enhancing technologies in the physical world that could be included in this category is as simple a development as barbed wire (McWhirter & Bible, 1992, p. 9). Recently, however, the European Union has had stricter privacy policies, especially regarding information concerning individuals, and the U.S. has had to make guarantees to the EU regarding the manner in which information about citizens of EU countries is to be stored and handled (Sullivan, 2006).

This literature review is a survey of the literature regarding current and recent American normative attitudes regarding privacy, with an emphasis on information and electronic monitoring. Other aspects of privacy are also explored. Current and previous policy is examined, and an examination of policy recommendations from the literature is conducted.

Although the emphasis of this review of the literature is on literature regarding privacy in the United States, literature regarding privacy policies in other western countries is also included. In some cases, countries are encountering issues which will arise in the United States in the future. These countries' academics' normative stances, particularly in Western Europe and the British Commonwealth, can be considered useful in constructing a review of norms and attitudes regarding privacy policy in a global context. This impingement of the global community on the United States therefore should be considered relevant to American public policy regarding privacy and consists of the development of a global culturally normative standpoint.

The literature can be categorized by the type of privacy which it addresses, and then by the date of publication. The date of publication will be broadly described as pre-9/11 and post-9/11. The pre-9/11 literature, unless specifically referencing the Twin Towers event, will be considered to consist of anything published up to

the end of 2001. This assumption is made based upon the length of time that papers generally spend prepress.

The literature regarding the Internet and Internet communication is specialized in the areas and scope of discussion of Internet communications. The literature can be grouped in various ways, and depending on the manner of categorization, some groups have overlapping subject matter. From the legal side, there was a major focus on the Fourth Amendment, as well as a special emphasis discussion of the invasion of privacy represented by the FBI's Carnivore program, as well as the possible illegality of its use, especially as there was no way to verify it was being used in the manner prescribed by law and by policy (Elmore, 2001).

The literature search revealed several Fourth Amendment treatments. Lawless (2007) focused on the privacy expectations of Internet search information. Barrett (2002) discussed the FBI claims that Carnivore collected information in the manner of pen register and trap-and-trace devices and the implications for Fourth Amendment protections for third parties, as well as the possibility the FBI was gathering more information with Carnivore than the courts may have allowed.

Jackson (1999), in a pre-9/11 piece, expressed concern that the Electronic Communications Privacy Act of 1986, while providing some protection for electronic communications, did not go far enough to protect individuals' privacy in electronic communications. The Harvard Law Review ("Keeping secrets," 1997) was concerned with the question of striking a balance between privacy, individuals avoiding suspicionless monitoring by law enforcement, and the necessity of law enforcement in cyberspace.

Another group of law journal articles discussed the Fourth Amendment specifically in terms of the FBI and Carnivore. Hellums (2002) is concerned with

the ability of the government, through the use of Carnivore and technologies similar to Carnivore, to fulfill Justice Brandeis' prediction., made *Olmstead v United States* in 1928, that "…the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." Young (2001) questions the FBI's use of the laws as old as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to justify the use of Carnivore. Lincecum (2003) references the movies "The Conversation" and "Enemy of the State" in illustrating the dangers of uncontrolled eavesdropping and the general distrust Americans have of government surveillance. Another closely related article (Ditzion, 2004) concerns the use of "pen registers" and what the law says that will be applicable to the use of pen register type surveillance in the Internet age, and how they relate to "trap-and-trace" devices.

Carnivore was a pre-9/11 invention by the FBI which evolved out of Omnivore, which itself evolved from a "still-classified surveillance system deemed technologically deficient" (Hellums, 2002, p. 2). The use or misuse of Carnivore hinged on what probable cause and court orders were necessary for its use, and the type of information to be collected. Levels of information could be considered as addresses email was sent from (to the target), addresses the target sent email to, address routing information and message contents. Conceptually, "pen registers" and "trap-and-trace devices" are carry forwards from the days in which circuit-switched telephone systems were used. Pen register and trap-and-trace technologies are analogous to and descriptive of the idea of inference tracking (E. Cole, 2003), in which knowing which parties are communicating with each other can give insight into who is up to something.

A pen register detects and records numbers dialed from a phone, and trap-and-trace tells those conducting surveillance from where a call was dialed to a certain number. In terms of email, these concepts were extended to the email address

and routing information. The burden of proof for getting pen register and trap-and-trace orders was less onerous than conducting a wiretap (i.e. a Title III order), which required more of a burden in terms of probable cause, and had time limits and other restrictions which law enforcement found to be inconvenient. For example, a Title III order "require[d] probable cause for intercepting communications' content or an ECPA order…" and "applications under Title III require the authorization of a high-level Department of Justice official and are subject to approval and review by federal district court judges" (Hellums, 2002, p. 3). These requirements were burdensome and time-consuming for the agency and were not given high priority, nor were sufficient resources devoted to the tasks.

Some of the controversy surrounding the use of Carnivore had to do with the FBI's implausible technical explanation for the manner in which Carnivore functions. The agency assured target audiences that the FBI was not intercepting the full content of a suspect's communication when the FBI was not authorized to do so. Because the workings of Carnivore were never divulged, some thought that it was implausible that the FBI could target specific email addresses for monitoring and analysis. Carnivore had other problems from civil libertarians' standpoints in terms of who would monitor the manner in which the software was installed and configured, as the software had capabilities built into it to collect all of the content information (i.e., the email message body). Carnivore also possessed the capability to monitor all traffic of all types (e. g., Web browsing, etc.), if the agency so desired.

In terms of the relevancy of any literature about Carnivore *per se* to the present day privacy issue, there is little. The USA PATRIOT Act has obviated the need for justification of surveillance which the FBI was compelled to show in the past. Surveillance of Americans of a much more comprehensive nature is now allowed and is authorized internally by the FBI through the use of National Security

Letters (NSLs). The FBI can issue NSLs by and to itself without a judicial oversight (Jordan, 2007). As the post-9/11 law review articles indicate, in terms of the normative view of the legal profession, as represented by the viewpoints expressed by their published advocates, there was concern in attempting to maintain privacy in email communications.

The current discussion regarding legal issues concerning the Fourth Amendment focus on the seizure of search results held at third-party search providers such as Google, Yahoo, etc., than other computer or data acquisition. The Lawless (2007) article urges judicial adoption of a rights-based doctrine in upholding societal expectations of privacy for constitutional consistency. Foley (2007) notes that the court in *Gonzalez v. Google* stated that even as the government sought search information which pertained to lawful activity, the tendency might be for the government to seek information about "suspicious activity" which would reveal the searcher's identity even if there was no previous reasonable suspicion. Goldberg (2005) notes that Google is the heavyweight in the world of Web search and free email, and privacy guarantees must be maintained lest the "electronic dossiers" which include records of all searches as well as all outgoing email from the free Gmail service would be sought at the very least by all manner of marketer.

In the aggregate, the issues discussed in these articles have to do with what expectation of privacy individuals have when conducting searches on the Internet. The search data is generally stored indefinitely at third-party search providers, such as Google, which says it never deletes any search query. Google search data has been seized and used by prosecutors. In one case, a man searched on a type of wound which he inflicted upon himself when he killed his wife and shot himself (non-fatally). The search history was evidence which ultimately proved to be his story's undoing, which was that an unknown assailant shot them and he lost consciousness (Lawless, 2007, pp. 1-2).

An observation from Lawless involves the tests that the courts apply when deciding if any “reasonable expectation of privacy” has any basis. In general, the basis of that expectation is tied to societal norms and guarantees the courts provide for individuals. The conundrum in these cases has to do with the fact that because third-party search providers do nothing to protect the queries entered into the search engine, that “it reinforces the privacy norms of a politically and temporally insulated judiciary: once people know their searches are exposed, then – by the time these cases are contested – there will, in truth, be no expectation of privacy” (Lawless, 2007, p. 8).

There is a paucity of law review articles regarding litigation concerning the USA PATRIOT Act. The fact that an individual must have standing (a legal term of art meaning they have to have some kind of interest caused by experiencing a direct effect of the law) to sue limits the type and number of cases which can be brought for unjust application of the act to victims of these abuses. Another reason to sue would be for the reason that an individual might consider application of the Act as a violation of that individual’s constitutional rights. The explanation used by the government is that any application of the Act is a secret affair. The penalties attached are against any individual who would divulge that they aided law enforcement in the execution of any order under the Act. This aspect of the law makes judicial review of the constitutionality of certain provisions moot. No one can show he(she) has standing so there is no one a court can be shown was harmed. The harm is kept a secret. The government’s claim that the plaintiff lacked standing led to the dismissal of a case in Cincinnati in July 2007. The court stated that the plaintiffs in the case, including lawyers and journalists, could not prove they had been subject to surveillance and therefore could not show injury, and therefore did not have standing to sue (Liptak, 2007).

Another tactic the government uses to keep issues out of court is to claim that there is some type of prejudicial harm that can come to security efforts if a judge

were to hear cases that involve secrecy and/or national security. This is currently the tactic being used in the case of *Al-Haramain v. Bush* in the United States District Court for the Northern District of California. This case is also the closest that plaintiffs have come to getting heard in court.

Al-Haramain is a charity that now is no more. It was shut down for suspicion of being involved in financing terrorists and terrorism. Joe Eisenberg is arguing on the side of the charity which claimed it had been given copies of its phone logs by the Treasury Department by accident. The papers Treasury turned over were marked “Top Secret” on each page. The FBI retrieved the packet of papers but not before several people in the law office had seen them.

When the warrantless surveillance program was revealed in December 2005, the attorneys for the charity realized what they had seen was evidence generated from that program and they filed suit (Elias, 2007). The government argued that “The Document,” as it is referred to in court papers, should not be entered into evidence or produced through discovery, as it was a state secret. The court let the suit proceed based on the recollection of a plaintiff who had seen it. The government argued that the only way to verify if the recollection was correct was to compare it to the Document, but since the Document would not be produced, the suit should be dismissed.

The Deputy Solicitor General Gregory Garre, in urging the judges to dismiss the lawsuit, said that exposing the Document, or even continuing with the case, would jeopardize the national security of the United States. When challenged as to whether the judiciary should just take the executive branch’s word that something should be considered a state secret, Garre suggested that the courts should show the “utmost deference” to the Bush administration (Poulsen, 2007).

The lengths to which the government goes to try to maintain the secrecy of the Document, notwithstanding the part about Treasury handing it over to the subject of their investigation, are extreme. Eisenberg must type his briefs on a government computer with an armed guard watching, cannot keep copies of what he's written, and any printouts he makes must be taken for shredding by the guard. As he wrote in an email:

> So, it's like this. Yesterday, under the auspices and control of my litigation adversaries, at their offices and on their computer, I wrote a brief, of which I was not allowed to keep a copy, responding to arguments which I was not permitted to see, which will be met by a reply which I will not be permitted to see. (Liptak, 2007, par.19)

A three-judge panel in a Washington appeals court did not like the government's approach to handling cases involving state secrets. Judge Judith W. Rogers, for the majority, wrote that the deck seemed stacked for the government in that when a plaintiff "lacks information about his claim, the complaint must be dismissed… But as soon as any information is acquired, it becomes too risky to introduce the evidence at trial" (Liptak, 2007, par. 16).

The government made a motion to dismiss in January, 2009 and it was denied in the al-Haramain case ("Order pertaining," 2009). There was a conference scheduled for January 23, 2009 ("Clerk's Notice in Al-Haramain Islamic Foundation, Inc. et. al. v. George W. Bush et. al.," 2009), and at that time the government was ordered to produce a plan by February 13 for going forward with the case, bearing in mind the sensitivity of the documents the court needed to see. On February 11 the government filed a brief with the court declaring its intention to appeal and get a stay. The court found that the decision to move forward with the case was not appealable. At the time of this writing, Judge Vaughn issued an order dated February 13, 2009, denying the government's motion to appeal and stay the court's order that the government produce the documents *in camera* that the court has determined that it must see in order to proceed with the case. The court has given the government until February 27,

2009 "…to inform the court how it intends to comply with the January 5 order" (Case 3:07-cv-00109-VRW, p. 3).

Another group of writers addresses the loss of privacy on the Internet in a general way, without focusing on the Fourth Amendment or Carnivore specifically, addressing the loss of privacy and government and commercial interests' infringement of individuals' civil rights generally (Smith, 2005; Bowie & Jamal, 2006; Freiwald, 2007; Reilly, 1999; Thompson, 1999; Skatoff-Gee, 1996; Glancy, 2000; Berman & Mulligan, 1999; Knopf, 1999; McTigue, 1999), and also employees' expectations of privacy at work (Dixon, 1997).

The Dixon piece is from the early days of the commercial Internet, and addressed employers' monitoring of employees' email communication. The use of email in the corporate environment was relatively new, and employees generally were under the impression that their expectation of privacy was similar in using email as to that expectation of privacy in making personal phone calls. The court ruled in *Smythe v Pillsbury* that no employee email had any protection. Dixon takes issue with this decision, maintaining that the court misread the societal expectation of privacy, and that from a culturally normative viewpoint, the employees should have been able to expect their email communications to be treated as private, much as personal phone calls in the workplace were protected.

According to Dixon, there existed an expectation of privacy in a wider sense. On the other side of the normative coin, the federal court's decision "is significant because it is the first federal decision to hold that a private sector at-will employee has no right of privacy in the contents of his or her email when it is sent over an employer's email system" (Dixon, 1997, p. 1). Dixon's argument is that if the employer gives the employee access to the public Internet via the

company network, and that employee uses some type of Web-based mail system, that employee has some expectation of privacy.

For post-9/11 considerations in terms of electronic communication privacy, Freiwald sums up the essential issues in a succinct, easy to understand manner. The courts had avoided addressing the constitutional issues surrounding wiretapping for 40 years. Two cases in 1967, *Katz v. United States* and *Berger v. New York*, established procedural safeguards to be placed on traditional wiretaps based on Fourth Amendment considerations. Since that time, however, the courts have not subjected modern electronic surveillance practices to constitutional scrutiny (Freiwald, 2007, p. 1).

Freiwald's piece raises the question of normative attitudes about privacy, as there are several unanswered questions about the government's surveillance in relation to the Constitution. The first case challenging, on constitutional grounds, the Stored Communications Act (SCA), which was passed as a subset of the Electronic Communications Protection Act (ECPA) in 1986, was pending at the time of publication in the Sixth Circuit (*Warshak v. United States*) (Freiwald, 2007, p. 2).

Freiwald hypothesizes as to the reason that there has been no constitutional review of any of this warrantless invasion of privacy by the government. She gives the reason simply as the fact that a test for users' reasonable expectation of privacy needs to be applied for the courts to rule on these issues, and that this is beyond the capability of the courts, in that they "lack adequate empirical data for the positive inquiry and adequate guidance for the normative one" (Freiwald, 2007, p. 2).

Subsequent to Freiwald's publication, the court did come down on the side of privacy, but only in that the police need search warrants to seize older emails

from ISPs. From the perspective of criminal defendants whom the police had a case against, the point of the ruling was practically moot, because the police needed warrants for newer mail. However, from the perspective of the general public, it was a good decision for privacy advocates because it limited the ability of the government to engage in warrantless fishing expeditions (“Warshak v. United States,” 2007).

The other selections in this grouping are consistent in that the selections from the pre-9/11 time period discuss privacy in a general fashion from several different angles. Privacy, and the compromise thereof, was described and discussed in terms encompassing such diverse activities as tracking down deadbeats, keeping the privacy of one’s images (in the suppression of distribution of a videotape on the Internet), increasing capabilities for monitoring users and considering the misperception that any communication can be considered private (McTigue, 1999).

McTigue makes a similar point to Freiwald’s, by describing cases in which people’s expectations of privacy in electronic communications were unfounded and the consequences deriving from these circumstances. One of these involved the case of Senior Chief Petty Officer Timothy McVeigh of the U.S. Navy, who was associated with his screen name by AOL employees in direct contravention of the company policy of non-disclosure on information about their subscribers (McTigue, 1999, p. 3). McVeigh was dismissed from the Navy because of the company’s disclosure of information of violation of its rules.

A major issue in the study and discussion of vacuuming up citizens’ emails had to do with the fact that the bars of the various states had not decided whether attorney-client communication could occur via email without encryption. This confusion as to the standards of confidentiality to which client communications should have been kept, appeared to fly in the face of knowledge the state bars

should have had regarding the problem for their clients with law enforcement copying and seizing stored emails (McTigue, 1999, p. 6). McTigue also arrives at a reason for the legal community's naivete concerning the difference between stored communication and intercepted communication in terms of maintaining attorney-client privilege. This naivete involves the fact that state bar associations focused on Title I of the ECPA which applies to email interception. In real-time, email interception is as difficult as wiretapping. Title II of the ECPA applies to the stored aspect of the email and because it is illegal to disclose stored information in an unauthorized fashion, the Act is of no consequence in helping to protect privileged communication. However, with the proper authorization, the attorney-client privilege cannot be maintained against the state without the use of some type of cryptographic protective measure. Title I is not relevant when it comes to the government seizing the stored communication per Title II (McTigue, 1999, p. 6) and in non-technical circles, this could lead to confusion.

The third group of articles regards possibly the most privacy destroying technologies available, physical tracking technology (Phillips, 2005; Caldwell, 2006; Glancy, 1995). The technologies in use now which allow cell phones to connect to any cell tower as the owner of the phone travels, and Global Positioning Systems (GPS), which allow people to do away with paper maps, are technologies which can be turned around and used to plot the location of anyone using these technologies at any time. These records are stored by the entities providing the services, and are considered "contentless" data. The question with these technologies has to do with whether a person has a reasonable expectation of privacy of location when employing these technologies.

Glancy (1995) clearly saw the coming future, as her publication was well before 9/11 and also before email was the ubiquitous application that it has become. All three authors are on the same side on these issues, that there should be an expectation of privacy when using these devices.

Caldwell argues the case for privacy very specifically from the point of view of the fact that the Florida Constitution specifically has a clause in Article I, Section 23 ("Florida constitution," 1968) enumerating the right to be left alone. This Right to Privacy parallels Fourth Amendment protection which itself is synchronized with the pre-9/11 federal interpretation of what the Fourth Amendment meant. He examines whether there is an expectation of privacy regarding cellular calls and how this means the 'Shaktman test,' a three part test to determine if a user has a reasonable expectation of privacy, applies. For these purposes, "…the state carries the burden of satisfying the three-part test of compelling state interest, relevance, and least intrusive means" ("Limbaugh v. Florida," 2004). What is interesting about the Limbaugh case in terms of the post-PATRIOT Act age is that it concerns Rush Limbaugh's medical records, which Limbaugh's attorneys contended were seized illegally from four of Limbaugh's physicians. The PATRIOT Act specifies that in terrorism investigations, the state can seize and use medical records without probable cause or a search warrant – that all the state must do is claim that it is germane to some investigation (Lenzer, 2006).

Another technology that Caldwell examines is implicated in the example of *Kyllo v United States*. In this case, the police used thermal imaging to detect drug activity inside a home. The Supreme Court argued that the police could not specifically use "sense-enhancing" technologies against random targets, or targets they intend to examine without a warrant, unless those techniques were in widespread use by the general public (Caldwell, 2006, p. 9). Unfortunately for privacy considerations of the general public, the cost of technology continues to go down, and therefore the chance of "widespread use" increases. The question specifically of what "widespread use" means is also subject to interpretation.

Glancy (1995) saw specifically the type of situation in which the logical conclusion is that each person ultimately would have to register their destination every time they were about to leave to go somewhere. Ostensibly, this type of

surveillance system would determine which roads to drive upon, and also allow for constant monitoring of the individual's location. The results of this monitoring could be stored in a database and correlated with the patterns given to private industry for more targeted marketing, and in the post-9/11 age, government.
Phillips (2005) discusses the set up and implementation of the E9-1-1 system in Texas, and how the raw data, basically the same information as in the previous two examples, could be used to build profiles of individuals who were being tracked. A simple move would be to say that the government would have access to this data and be able to build location/identity databases for any reason, of which one could be anti-terrorism tracking. Anti-terrorism would not be the only use.

There have been differing rulings as to the question of whether the government can seize cell phone location records and/or get real time cell phone location data without a warrant. As recently as 2005, there were differing opinions in federal courts in terms of what Fourth Amendment protections applied to those data. In five cases in 2005, two judges treated the request for real time data as an order for a tracking device, two treated them as wiretaps and another held it was the same as a pen register order (the order with the least protection for the target). This part of the law is still evolving ("Government requests," 2006).

### 1.3.1. Americans' Attitudes Regarding Privacy

Davis and Silver (2004) conducted a survey in the aftermath of the 9/11 attacks. The telephone survey was conducted between November 14, 2001 and January 15, 2002 and surveyed 1,448 respondents.

There were nine questions which the research was predicated on. The answers to these indicated the respondent's choice between preferring security and

preferring civil liberties. The population included an over-sample of African-Americans and Hispanics.

The questions postulated situations in which the respondent had to make a choice. In the case of the innocuous “Give up some civil liberties” entry in the table, the respondent would be asked if they would be willing to give up some civil liberties if it would make the country safer. If the respondent answered yes, the respondent would be categorized for that question as preferring security to civil liberties. For the table entry for results for “Crime to belong to a terrorist organization,” the question was posed and the answer categorized in the following way:

> In [the] Survey, when the value trade-off is framed as the need to be safe and secure against judging people guilty by association – “people who belong to or associate with terrorist organizations should be considered a terrorist” – 71% support treating people as guilty based on their associations. (Davis & Silver, 2004, p. 32)

Some of the situations in the middle range of acceptance/non-acceptance, in terms of what respondents preferred, were yielded by posing privacy destroying actions such as “Warrantless searches on suspicion” and “Monitor telephone and email.” Even in the initial post-9/11 hysteria and fear, most people voted to protect civil liberties the majority of the time. Additionally, “Investigate protesters” received only 8% agreement for a security response, with 92% taking the civil liberties side. This is in line with Chomsky’s observation that both political parties are to the right of the populations they “serve” (Chomsky & Matta, 2008).

Warrantless searches received only 23% approval, and monitoring telephone and email received only 34% agreement in terms of the security responses. Thus it is evident via self-reporting that the societal norm in American’s minds is for a free society even in the immediate aftermath of a terrorist attack (Davis & Silver, 2004).

### 1.3.2. Conclusions from the Literature

The conclusions that can be drawn from the literature involve the observation that even in a shell-shocked state, immediately after the attacks of 9/11, the American public was only slightly in favor of giving up some of their civil liberties in return for security. In regards to anti-war protest groups, Americans did not favor suppressing political dissent.

The inferences that can be drawn from the literature on the legal side of the question include that the normative cultural value of Americans regarding privacy was such that Americans favored having privacy, and wanted to keep what they thought they had of it. The events of 9/11 changed the focus of the discussion. The playing field for privacy rights tilted so much in favor of the government that it seems to have become difficult for scholars and privacy advocates to decide about which privacy destroying initiatives to write because there were so many.

Post-9/11, the standards the government had to meet and the requirements necessary for safeguarding civil rights changed overnight with the passage of the USA PATRIOT Act and the other acts complementing it. This changed the tone and direction of the privacy debate, by making privacy and civil rights advocates start much further away from the positions they could reasonably expect to defend. The right to privacy had been built up over the years by degrees with court rulings establishing and expanding the right. Strict constitutionalists could reasonably maintain that there was no need to establish the right to privacy because the Constitution didn't grant the federal government the power to decide if we should or should not have privacy.

The main battlegrounds in the privacy war are battles over email seizure, email monitoring, Web surfing and location tracking and the associated profiling which the organization of all of the data about an individual would yield.

Americans still want and value their privacy; however there are serious problems for those who care about personal privacy and liberty. This is brought about by the manner in which the government conducts surveillance.

### 1.3.3. Privacy and the Law

The events of September 11, 2001, precipitated the passage of laws which have become flashpoints in the discussion regarding privacy. These laws figure prominently in the literature regarding attitudes toward privacy as elucidated in various authors' offerings on the subject. Americans' attitudes toward privacy are important due in part to the shift in focus on the part of intelligence and law enforcement agencies toward prevention of terrorism as a goal and away from apprehension and prosecution of terrorists after the terrorist act has been committed. These laws are the tools the government claims as necessary to conduct the surveillance necessary to combat terrorism.

The primary law in question is The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. The Act was signed into law on October 26, 2001.(*Report from the field*, 2004) The Act has subsequently been renewed, with revisions and expansion of the government's powers, as there were some sunset provisions in the Act as a protection for civil liberties. Those sunset provisions were nullified by the provisions of the Act as extended and expanded with the signing of HR 2417 "Intelligence Authorization Act for Fiscal Year 2004" (Bush, 2003) on December 13, 2003, HR 3199 "USA PATRIOT Improvement and Reauthorization Act of 2005" on March 13, 2006, and S2271 "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006" on the same day ("Statement on HR 199," 2006). The earlier laws were precursors to the Real ID Act, which was signed into law on May 11, 2005. The laws signed after 2005, which increased

the power of government, can all be considered to be cut from the same cloth, including the FISA Amendments Act of 2008, PL 110-261.

Sections of these laws included budgetary provisions and increased penalties for various terrorist related offenses. Those sections are not germane to the discussion here. The sections of the laws of concern in this literature review relate to the expanded powers the government granted to its intelligence and law enforcement agencies in the government's surveillance of all citizens and individuals in general, within the confines of the United States. Many of these powers can be exercised with little or no oversight and many can be exercised without any judicial review.

The lack of judicial review is a theme in literature regarding Fourth Amendment rights and the traditional 'probable cause' theory in the law. The Fourth Amendment is the amendment which proscribes "unreasonable searches and seizures."

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. ("Bill of Rights," 1791)

The full text of the Fourth Amendment is included here to demonstrate that as technology has evolved, the language of the Constitution must be interpreted according to the intent of those who framed the Constitution for this amendment to be relevant.

Application of the USA PATRIOT Act also has Fifth Amendment (right against self-incrimination) ramifications. Additional fallout from the Global War on Terror (GWOT – this is an operational term used by the Bush Administration to describe operations against terrorism) include possible Sixth Amendment (speedy trial,

right to confront accuser) and Eighth Amendment (cruel and unusual punishment) issues.

The use of these laws impinges on the First Amendment rights of individuals, which leads directly to the abridgement of rights that the Real ID Act represents. The Real ID Act was passed for the reason of providing a framework requiring verification of identity of U.S. persons and therefore providing security for society by that guarantee of identity of individuals carrying these Real IDs.

What the use of Real IDs will mostly accomplish will be to establish a single point of identity for tracking citizens throughout their daily lives. Tracking citizens will become easier to do than it is currently, as the initial specification of the Real ID RFID mandates that citizens' information is stored on the card in unencrypted form. Additionally, the current specification and implementation of "enhanced drivers' licenses" (EDLs) requires no security features. In this way, anyone with an RFID reader can read the information on the EDL. DHS has previously dismissed security concerns about the EDL and Real ID security flaws as an academic exercise, and has stated the department will do nothing to enhance the security of the Real ID and EDLs. Recently however, a security researcher drove around downtown San Francisco streets harvesting EDLs and passport numbers using $250 of commercial off the shelf (COTS) technology. According to the researcher, he wanted to provide a proof-of-concept demonstration that what researchers said could be done, could in actuality be done (Goodin, 2009).

This lack of security of the information on the IDs may seem counterintuitive, yet the manner in which the Real IDs are set up to be implemented provides for plain text storage of data. The original specification was for RFID, and there is nothing to keep DHS from specifying the RFID implementation in the future. The current rules for implementation dictates a 2D bar code on the actual ID card, but there is no change in the database aspect, in which a massive database, maintained by

each state but interconnected as a distributed database, will maintain the basic identity information of each individual (*Minimum standards*, 2008).

The inclusion of this background on the effect of Real ID should underscore the importance of the issue of privacy. This is because the right to privacy, although not written into the Constitution, was derived from reading the intent of the Constitution by various Supreme Courts and formed the basis for decisions rendered based on those readings. Thus the rights to privacy are built on fundamental rights of the people guaranteed in the Constitution.

### 1.3.4. The Public Discourse and Societal Norms Regarding Privacy

The largest shift in the nature of the public discourse regarding privacy occurred with an incident of international terrorism. The U.S. Governments stated the need to protect its citizens and itself from international and domestic terrorists. In the United States, the events of 9/11 were the catalyst for major changes in the way privacy was regarded and implemented ("USA PATRIOT Act," 2001).

Prior to 9/11, there had been serious discussion within the computer profession regarding the manner in which individuals' information should be handled by the government and commercial entities. Generally industry actors would act according to a rational choice (for corporate actors) model when it came to the collection and use of individuals' information. The corporate actors would attempt to maximize the profit realized from collecting and brokering the personal information they collected, while doing the minimum possible to safeguard the information. Milberg (1995) examined the issues and concluded that corporate actors would do well to protect the information of the individuals whose information they collected, lest citizen and consumer concern trigger some level of regulatory remedy. They also found an overriding consideration may have be work, that information privacy could be considered a "hypernorm," transcending

cultures and fundamental element in human existence - thereby creating an ethical imperative for the information's protection (Milberg, Burke, Smith, & Kallman, 1995, p. 73).

Froomkin (2000) expresses concern over how little control individuals can exercise over their information once it is in a database. Froomkin's initial solution is for individuals to attempt to limit the amount of information they hand over to marketers and the government. Froomkin discusses the "media-sanctioned exhibitionism and voyeurism" in society and observes that some might think it reactionary to worry about information privacy under those circumstances (p. 1466).

One observation regards the categorization of privacy-destroying technologies, into technologies which "facilitate the acquisition of raw data and those that allow one to process and collate that data in interesting ways" (Froomkin, 2000, p. 1468). The contention and the argument developed regard the difference between data that might be collected for a single purpose and not parsed to associate with an individual, and data that is collected for aggregation and association with specific individuals. The latter type of data, that which can be associated with an individual, can provide the foundation for or additional information to aid in the development of personal profiles. In the endgame of information acquisition, the questions of prediction and predictive abilities are paramount. This is the case with the NSA's "Advanced QUestioning Answering for INTelligence," or Aquaint program (Bamford, 2008). Aquaint is the most advanced and modern profiling and prediction tool possessed by the agency. NSA also has, especially for the warrantless wiretapping aspect of the operation, a slew of social network analysis, data mining and traffic analysis tools. All of these need information as input, but the tools aggregate and analyze the data (Bamford, 2008, p. 149), associating it with specific individuals and building profiles, in the manner that Froomkin described in his pre-9/11 work.

Post September 11, policies regarding privacy would take two roads simultaneously. The first road involved the continuation of the public discussion regarding privacy in the sense that it had been conducted pre-9/11 in terms of local law enforcement and commercial interests. The second road involved the discussion of privacy in the context of anti-terrorism and national security.

An example of the post-9/11 privacy concern, as well as the public (government)-private surveillance partnership, is illustrated in the case of Lakehead University in Thunder Bay, Ontario. In this case, concerns over the PATRIOT Act and the powers of the U.S. government to harvest data off servers in the United States made faculty at the university wary of the use of Google's products and services.

Michael Pawlowski, vice president of administration and finance, defended the university's decision to allow Google to build out a new email and collaborative tool system for the university, at no cost to Lakehead. The downside was that the system could not be used to transmit any private data, including students' grades. The PATRIOT Act gives the U.S. government the authority to "secretly view data held by U.S. organizations." This type of activity is contrary to Canadian privacy laws, which requires individuals to be notified when their data is shared and also that organizations protect individuals' data.

Tom Puk, a former president of the faculty association at Lakehead, elaborated on the grievance that the faculty association filed with the university, saying, "By getting this free from Google, they gave away our rights." Darren Meister, associate professor of information systems at the Richard Ivey School of Business, observing the disconnect between Canada's privacy laws and the United States' security measures, noted that in terms of Canadian organizations making the decision to allow their data to reside on U.S. servers, "You have to decide which law you are going to break."

As Mr. Puk observed, the PATRIOT Act allows the U.S. government to scan all the information held on the servers it can secretly examine, and then build profiles based on the writings found there. This could be a problem for academic freedom in Mr. Puk's estimation, as individuals might be researching something that might end up getting them disqualified for entry into the U.S. (Avery, 2008). Various academics and researchers have been denied entry to the U.S. even as they were scheduled to give presentations at conferences, so the fear is not entirely groundless (Keizer, 2007).

Google maintains that it makes valiant efforts to protect customer records, although there is some debate on that point. Specifically its policies on anonymization of user data allow the data to be easily recovered in one step (Metz, 2008), and it is also providing the Center for Disease Control with data regarding user searches, ostensibly to help the U.S. government locate flu outbreaks (Helft, 2008).

### 1.4. Government's Assumption of Extraordinary Power

In history in the United States, during times of war and national emergency the Congress passed laws that restricted personal liberty for national security reasons. Enforcement of these laws can be seen as abridgements to and restrictions of enumerated rights, including such First Amendment rights as the freedoms of speech, assembly and association. Wartime has also been used as the reason for using a conceptually different framework for deciding the manner in which crime and punishment are defined. Thus, in World War II, military tribunals for foreign enemy combatants were instantiated and upheld by the Supreme Court in *Johnson v. Eisentrager* (Posner, 2006, p. 57). The issues of crime and punishment in times of the abridgement of enumerated Constitutional rights impinge directly on privacy in terms of the Fourth Amendment as a protection against privacy-destroying surveillance. For example, during World

War I, the government encouraged citizens to report on their fellow citizens in cases of speech or action that might be interpreted as disloyalty to the government. As some speech was illegal, Fourth Amendment guarantees against unreasonable search and seizure conflict with the idea that speaking privately to another private individual (i.e., not law enforcement personnel) might result having that speech used as evidence against the speaker. In cases of three or more individuals gathered, it would also impinge on the enumerated First Amendment right of freedom of assembly.

### 1.4.1. Alien and Sedition Acts

The first instance of legislating restrictions on personal freedom because of national emergency came in 1798, with the passage of the Alien and Sedition Acts. These consisted of the Naturalization Act, the Alien Friends Act, the Alien Enemies Act and the Sedition Act.

Europe was in the throes of war, with the countries of France and England at war with each other. The United States was reluctant to join the conflict on either side, hoping to remain neutral. However, the French were seizing and sinking American merchant ships. These ships, the French claimed, were thought to have been conducting trade with Britain. The situation has been characterized as an undeclared naval war with France (Smelser, 1954).

The Alien Friends act was enacted because of the fear that non-citizens (aliens) might be disloyal and therefore these aliens represented a danger to the Republic. The Alien Act gave the President power to detain and deport any non-citizen who was considered to possibly pose a danger to the United States ("Alien Act of 1798," 1798).

The Sedition Act of 1798 prohibited the publication of “any false, scandalous, and malicious writing” against the government of the United States or the institutions of the Executive or legislature. Enforcement of this Act could be seen as a *prima facie* abridgement of First Amendment freedoms. The Sedition Act was successfully used to prosecute any individuals who dissented and stirred up opinion against the Adams administration. The Act expired on Adams’ last day in office and Jefferson pardoned those who had been convicted under the Act (Stone, 2003).

### 1.4.2. The Civil War – Habeas Corpus

The Civil War, being a time of war and national emergency, led to some abridgements of traditional protections under the law in the name of national security. A notable example of this abridgement was the suspension of the writ of *habeas corpus*.

President Lincoln, soon after taking office in 1861, had considered and then rejected the idea of preventing the Maryland state legislature from meeting on April 26th. There was a legitimate concern that Maryland would vote to secede from the Union, thereby isolating Washington, D.C. (Halbert, 1958).

Soon after hostilities started with the attack on Fort Sumter, the Sixth Massachusetts Volunteers were attacked by a mob of Confederate sympathizers as they marched through Baltimore on their way to the capital. The Massachusetts militia arrived in Washington on the 19th of April. The attack by the mob and the subsequent rioting left sixteen dead and there was much damage to the city. The mayor of Baltimore then ordered the destruction of the bridges connecting Baltimore to the Union to prevent more Union troops from entering the city (Stone, 2003).

Under these circumstances, President Lincoln was still reluctant to suspend habeas corpus, yet he understood that he must take steps to prevent Maryland from seceding. The President decided to wait and see what the state of Maryland would do.

The President declared in orders to General Winfield Scott on April 25th, 1861, that if Maryland were to secede, General Scott should bombard their cities “if necessary,” and “in the extremest necessity,” suspend the writ of habeas corpus. Even though many of the people of Maryland had secessionist sympathies, these orders proved to be prudent in that Maryland never seceded (Halbert, 1958).

On April 27th, President Lincoln ordered the suspension of the writ of habeas corpus in an area along the line of the military front, drawn from Philadelphia and Washington, via Perryville, Annapolis City and Annapolis Junction. It was in this area that John Merryman operated (Halbert, 1958).

John Merryman had raised a company of soldiers for the Confederates and started drilling them. Merryman and these recruits were in possession of arms and Merryman was thus committing treason. On May 25, 1861, Merryman was arrested for “various acts of treason…” and held at Fort McHenry (Halbert, 1958). Merryman filed a writ of habeas corpus, and the petition was assigned to Chief Justice Robert Taney, a strict constitutionalist from the south, who ruled in Merryman’s favor, i.e., ruling that only Congress had the authorization to suspend habeas corpus, and therefore President Lincoln’s orders were illegal. In the end, the President ignored the Court. The New York Times attacked Justice Taney for making an “officious and improper” decision as it “presents the ungracious spectacle” of the judge wishing to “exculpate a traitor” (Stone, 2003).

President Lincoln explained his rationale for suspending the writ by stating famously that Judge Taney’s decision would allow “all the laws, but one, to go

unexecuted, and the Government itself go to piece, lest that one be violated." A few weeks later, the President suspended the writ in Florida.

President Lincoln suspended the writ of habeas corpus on eight separate occasions, including the most extreme suspension order, a nationwide suspension which declared that "[A]ll persons…guilty of any disloyal practice…shall be subject to martial law." In 1863, the Congress legislated the President's actions into law. The Democratic press widely quoted William Seward when Seward told the British minister in Washington that, "I can touch a bell on my right hand and order the arrest of a citizen in Ohio. I can touch the bell again and order the imprisonment of a citizen of New York, and no power on earth but that of the President can release them. Can the Queen of England, in her dominions, say as much" (Stone, 2003, p. 222)?

After the war, the writ of habeas corpus was restored.

### 1.4.3. World War I – The Espionage and Sedition Acts

In April 1917, the United States entered the war in Europe and public opinion was divided as to whether the United States should participate in the war in Europe. Many citizens believed the motives behind the United States' entry into the war were less than pure, and that the United States was going to war to protect wealthy individuals' investments. Nebraska Senator Frank Norris said, "[W]e are about to put a dollar sign upon the American flag." President Wilson was not of the mind to allow this type of dissent. He declared that disloyalty "must be crushed out" and that disloyal individuals "had sacrificed their right to civil liberties" (Stone, 2003).

The Espionage Act of 1917 was primarily concerned with espionage and sabotage. Other provisions of the Act had consequences for free speech.

Specifically, any speech of the nature that could be considered to obstruct recruiting or enlistment in the armed forces was restricted. Anti-war speech and dissent regarding governmental policy was therefore considered to be an attempt to discourage enlistment. Attorney General Charles Gregory declared in November 1917, referring to those who dissented regarding the war, “May God have mercy on them, for they need expect none from an outraged people and an avenging government.” (Stone, 2003, p. 223)

Initially, as prosecutions under the Act were being ramped up, three important Espionage Act cases were prosecuted. These cases involved Charles Schenck in one case, Jacob Frohwerk in another and Eugene Debs in a third. The briefs were written and submitted by Alfred Bettman, special assistant to the Attorney General in charge of prosecution under the Espionage Act.

Schenck was the general secretary of the Philadelphia Socialist party and published 15,000 anti-war leaflets. Some leaflets were mailed to men who were subsequently drafted. The pamphlets, among other things, urged the readers to “assert and support your rights” by upholding “democracy.” Justice Oliver Wendell Holmes, after reviewing the content of the leaflet, determined that Schenck would not have printed and circulated the leaflet unless he had intended it to have the effect of causing men to resist the draft, and upheld the conviction. It was in this case that Holmes applied the “clear and present danger” test to speech (Johnson, 1958, p. 472).

In the space of a single year, Justice Holmes went from a conservative interpretation of “clear and present danger” to a more libertarian interpretation. Thus in the early free speech opinions, he interpreted “clear and present danger” in the context of the common law crime of seditious libel, which turned on any utterance or printed word which criticized the “form, officers, conduct or policies of the government if such criticism could be construed” as painting the

government in a bad light or disturbing the peace (Ragan, 1971, p. 25). In these cases, the question of freedom of speech revolved around the question of “prior restraint,” the idea that the government could stop the printing or distribution of printed material, or the speech of an individual before the act, but that once the speech act had occurred, the government, as willed by the public, could determine whether the speech was offensive to public sensibility and thus be punished.

The test Justice Holmes was to employ in later cases involved a proximity test, which meant that some type of direct correlation between the speech and some type of incitement to criminal behavior needed to be shown. Much of the free speech debate from the end of 1919 on revolved around the question of the nature and scope of First Amendment protections and what utterances were protected speech and what were considered subject to governmental control during times of national crisis (Ragan, 1971, p. 40).

Another early Espionage Act case the Supreme Court heard was that of Frohwerk, editor of the *Missouri Staats Zeitung*. He was charged with writing thirteen anti-war articles published between July and December 1917. The brief Bettman submitted argued that the “main tenor” of the articles was “that Germany committed no wrong against the United States; that this country entered into the war for the benefit of England and the rich men; that the official reasons for our entrance into the war, such as the benefit of democracy and wrongs committed against us by Germany, are mere pretenses” (Ragan, 1971, p. 32). Justice Oliver Wendell Holmes of the Supreme Court wrote in upholding the Frohwerk conviction that “it is impossible to say that it [the court record] might not have been found that the circulation of the paper was in quarters where a little breath would be enough to kindle a flame” of resistance (Ragan, 1971, p. 35).

In the Debs case, the conviction was based on a speech that Debs gave June 16, 1918, in Canton, Ohio. Eugene Debs was well known, having received a million votes in his run as a Socialist for President in 1912 (Stone, 2003). In a speech Debs stated that wars were declared by the “master class” and fought by the “subject class”: “The master class has had all to gain and nothing to lose, while the subject class has had nothing to gain and all to lose – especially their lives” (Ragan, 1971, p.32). During the speech, Justice Department agents were able to gather evidence that men of draft age were present. The presence of those draft age individuals provided the basis for the government’s prosecution of Debs.

In this decision, Justice Holmes determined that Debs’ intent could be inferred from the Socialist party’s St. Louis platform opposing the war. Noting that the jury had been instructed not to hate the speech but to determine if the speech was calculated to bring resistance to the draft or the war and Justice Holmes determined that the jury, in convicting Debs, had discharged its duty properly.

The Espionage Act was used to prosecute people nobody had ever heard of. One of those individuals was Mollie Steimer, a Russian-Jewish émigré who handed out anti-war leaflets in Yiddish on New York’s East Side. This stifling of dissent for national security purposes may have been considered necessary for the security of the state at the time.

Some judges who had been against the application of the Espionage Act, started to pen decisions that viewed free speech rights more liberally. This included such judges as Learned Hand in New York and Justice Holmes, as well as Judges Bourquin and Amidon (Stone, 2003).

To remedy this situation, Congress passed the Sedition Act of 1918. This Act made it criminal, among other things, for “any person to utter, print, write, or

publish any disloyal, profane, scurrilous, or abusive language intended to cause contempt or scorn for the form of government of the United States, the Constitution, or the flag, or to utter any words supporting the cause of any country at war with the United States or opposing the cause of the United States" (Stone, 2003, p. 227).

After the war, the Russian Revolution was determined to be a danger to the United States, and Attorney General A. Mitchell Palmer formed the General Intelligence Division (GID) within the FBI to investigate radicals and radical activities. The GID conducted raids in 33 cities, arresting more than 5,000 on suspicion of radicalism. Attorney General Palmer reported that the "alien filth" the GID had captured were individuals with "sly and crafty eyes… lopsided faces, sloping brows and misshapen features" and that their minds were filled with "cupidity, cruelty… and crime." Over 1,000 of these individuals were summarily deported (Stone, 2003, p. 228).

Some observers after the war tried to make sense of freedom of speech in wartime. Speaking of the First Amendment, one author wrote, "If the sinews of out political body cannot bear the strain of war, they fail of their fundamental purpose… If our creed is merely a peace-time panacea, it is wholly unfitted to exist. For the world is forever at war" (Garrett, 1919, pp. 72-73).

In the end, the Red menace was defeated, and in 1920 Congress repealed the Sedition Act.

### 1.4.4. World War II – The Smith Act and Japanese Detentions

One and a half years before the December 7, 1941 attack on Pearl Harbor and the United States entry into World War II, on June 28, 1940, President Roosevelt signed into law what was commonly known at the time as the Smith Act. The

Alien Registration Act of 1940, or Smith Act, had several provisions, including making it illegal to advocate overthrowing the U.S. government by force or violence, being a member of an organization which advocated such violence, or conspiring to do so. There were only a couple of prosecutions during World War II. The first involved 18 members of the Socialist Workers party in 1941, and the second, 28 pro-Nazi individuals in 1942. In the second trial, the judge died seven months into the trial and it was never revisited and therefore was dismissed for failure to prosecute (Johnson, 1958, p. 469).

After the War, in 1949, 11 Communists were convicted under the Act in federal court in New York City of conspiracy to overthrow the government. The Supreme Court sustained the convictions of Dennis and his associates in 1951, and therefore sustained the Act's validity. This decision cleared the way for prosecution of Communists. The government vigorously pursued Communists in order to safeguard the Homeland. By 1956, 131 persons had been indicted, and 98 of those were convicted, 9 acquitted and 24 trials resulted in no verdict by the juries (Johnson, 1958).

In the case of Dennis, the Supreme Court upheld the Act because the Act prohibited advocacy, not speech per se. So an academic discussion of Marxism was permitted, but to advocate action against the government was illegal. This finding was in line with the Court's finding in the earlier case, *Schenck v. United States*. In *Schenck*, Justice Holmes in the majority decision affirmed that if the advocate's speech presented "a clear and present danger" then it was actionable. This rule was then modified to be a rule of "clear and probable" danger in Dennis, and under that legal theory, the rhetorical speech act of *Dennis* and his associates was actionable under the statute (Johnson, 1958).

The Supreme Court in 1957 heard *Yates v. United States*, in which the Court narrowed the definition of advocacy and allowed many Communists to escape

prosecution. The Court decided that there should be some sufficiency of evidence of anti-government speech before convicting an individual. The fact of Dennis being a leader of the Communist Party was evidentially sufficient to convict back in the late 1940s. The new view of the 1950s Court was that being a leader of an organization dedicated to the overthrow of the United States government was not enough to convict without evidence of the proscribed speech (Johnson, 1958).

On a parallel timeline, on February 19, 1942, President Roosevelt signed Executive Order 9066. This order effectively set up the Japanese internment camps. Neither the words Japanese nor Japanese-American appeared in the order, yet the effect was that in 1942, 120,000 persons of Japanese descent were resettled. Two-thirds of these were American citizens, and the total represented 90% of the total of all Japanese-Americans. In *Korematsu v. United States* in 1944, the Supreme Court upheld the actions in interring the Japanese Americans in terms of national security. Justice Hugo Black wrote for the majority, “Hardships are part of war, and war is an aggregation of hardships” (Lofgren, 2005).

The Japanese-Americans were released at the end of the war, and those who lived long enough received reparations payments from the government during the Reagan administration (Yoo, 1996, p. 684).

### 1.4.5. Cold War & Korea – McCarran-Walters and Communist Control

During the Korean Conflict, the Congress passed the Immigration and Nationality Act of 1952, more popularly known as the McCarran-Walters Act. This Act reformed the immigration laws and created a single referential law for immigration into the country. The Act gave the Attorney General wide discretionary powers on issues of deportation and allowed the Attorney General

broad authority in the matter of waiving restrictions on exclusion of aliens whom the Congress may have intended to exclude (Bennett, 1966).

Additionally, there were provisions in the Act which allowed the government to strip citizens of their citizenship for various offenses (Graham, 2005). The Act had provisions for denying visas and expediting the deportation of resident aliens. Chief among these offenses was if in individual was a member of the Communist Party, or if the individual in any way helped enemies of the United States with money or other aid (Margolick, 1982).

In 1954, Congress passed the Communist Control Act. This Act outlawed the Communist Party. Other measures were also put in place for the national security – including extensive loyalty programs and infiltration of subversive organizations (Goldstein, 2006; Marx, 1974). It was also during this time that the House Un-American Activities Committee investigated various individuals' political affiliations (Carr, 1951).

### 1.4.6. The Vietnam War

The Vietnam War era brought nothing new in terms of legislation to limit personal freedom. The state determined that the main dangers to the established order (the Establishment) at that time were the civil rights and anti-war movements. The groups were infiltrated and put under surveillance through undercover work.

J. Edgar Hoover launched COINTELPRO in 1956, and the FBI operated against dissident groups – and encompassed operations against socialist, white hate, black nationalist, civil rights, antiwar and New Left groups. These operations were able to achieve their objectives until 1976, when the Senate moved to limit domestic security activities (Garrow, 1988).

## 1.5. The PATRIOT Act

September 11 precipitated the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. The Act was signed into law on October 26, 2001. There were some sunset provisions in the Act as a protection for civil liberties. The Act has subsequently been renewed, with revisions and expansion of the government's powers. Many of the sunset provisions were nullified by the extension and expansion of provisions of the Act with the signing of HR 2417 "Intelligence Authorization Act for Fiscal Year 2004" (Bush, 2003) on December 13, 2003, HR 3199 "USA PATRIOT Improvement and Reauthorization Act of 2005" on March 13, 2006, and S2271 "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006" on the same day ("Statement on HR 199," 2006). (The reference is correct, on the White House Web site, the title was as it is printed here).

The PATRIOT Act grants intelligence agencies the ability to monitor communications, conduct searches of United States citizens' residences without informing the target of the search, and gather any manner of information without any judicial oversight. This means that searches can be conducted without the issue of a warrant based on probable cause (Jordan, 2007).

The vehicle of choice for seizure of all types of records is the issue of a National Security Letter (NSL). The NSL allows the FBI to go to a business and obtain any information for which the FBI asks. No judge is required for the issuance of a NSL. There are some guidelines. Additionally, in "emergency" situations, the FBI is allowed to seize information using an "exigent letter." These exigent letters are also only to be issued after some type of procedure is followed (Jordan, 2007).

An audit by the Justice Department Inspector General Glenn A. Fine uncovered irregularities in the FBI's following of its own procedures for issuing National

Security Letters. The FBI underreported the number of letters issued by 22%, some letters were used for improper purposes, exigent letters were issued without proper authorization, and according to the FBI's own count, at least 26 instances of the issue of NSLs were in violation of the procedures the FBI itself enumerated (Jordan, 2007).

The PATRIOT Act authorizes intelligence and domestic surveillance agencies to turn over the information gathered without probable cause to prosecutors. The prosecutors can then use the evidence in the prosecution of ordinary criminal cases. The custodians of the records who surrendered those records are prohibited from informing anyone (especially the target of what in the past would have been an illegal search) that they surrendered those records (Dunham, 2005).

The PATRIOT Act received a boost on December 13, 2003, with the signing into law of the Intelligence Authorization Act for Fiscal Year 2004. As Andrew Napolitano wrote on March 5, 2004, for the Wall Street Journal:

> This statute expands the term "financial institution" so as to include travel agencies and car dealers, casinos and hotels, real estate and insurance agents and lawyers, newsstands and pawn brokers, and even the Post Office. (par. 4)

When these powers are used against U.S. citizens in cases which do not involve national security, the Constitution's Fourth Amendment guarantees against unreasonable searches have been circumvented, in that no warrant is issued. No judge must determine if there is reasonable cause. In the past, a search required a search warrant specifying the place to be searched and the thing to be seized.

To illustrate the scope of the powers the government was interested in granting to itself, one needs only look at the events of early 2003 in the quest to pass the next generation of surveillance law.

In January 2003 the Justice Department created “The Domestic Security and Enhancement Act” which was sent to Congressmen on the Hill, but not to the full Congress at the time. A Congressional staffer had leaked the document to the press. When asked about the leaked document, a Justice Department spokesman, Mark Corallo, told the Village Voice that the legislation would be “filling in the holes” in the original USA PATRIOT Act, and would be “refining things that will enable us to do our job.” The circulation of the draft with proposals for over 100 new provisions was attributed to Attorney General John Ashcroft (Welch, 2003).

The public debate and controversy which ensued resulted in some setbacks in expanding the powers of the USA PATRIOT Act. At the time, Attorney General Ashcroft “denied a bill was in the works, although he admitted that the leaked document is ‘what we’ve been thinking’” ("EFF Analysis," n.d.).

One of the features the draft Domestic Security and Enhancement Act would have indemnified law enforcement and intelligence officials from being prosecuted for violating federal law when conducting these warrantless wiretaps or illegal searches as long as the officers were only following orders. Subsequent to the leak regarding the President’s authorization of warrantless wiretaps by the NSA in late 2001, observers reached the conclusion that the draft legislation leaked in 2003 was an attempt to legalize the NSA warrantless wiretapping program (Welch, 2003).

The Administration later claimed that the draft legislation leaked in January 2003 was not the legislation that the Administration wanted. According to Justice Department spokesperson Tasia Scolinos, “These proposals were drafted by junior staffers and never formally presented to the attorney general or the White House. They were not drafted with the NSA program in mind” (Eggen, 2006).

# CHAPTER 2. FOUNDATIONAL THEORY OF SURVEILLANCE

The reason given for the types of surveillance that the government conducts against American citizens involves the desire to avert another terrorist attack such as 9/11. According to former Attorney General John Ashcroft, President Bush told him, “Don’t ever let this happen again” (Solomon, 2006).

The advocates of the total surveillance regime that the U.S. government is in the process of imposing on the population of the United States argue that there is a logically straight line from the destruction of personal privacy protections under the Constitution to the prevention of terrorism. Conversely, it can be stated that the manner in which terrorism can be best prevented is to put every person under surveillance. The analogy is made by one of John Poindexter’s associates, Ted Senator:

> Our task is akin to finding dangerous groups of needles hidden in stacks of needle pieces. This is much harder than simply finding needles in a haystack: we have to search through many stacks, not just one; we do not have a contrast between shiny, hard needles and dull, fragile hay; we have many ways of putting the pieces together into individual needles and the needles into groups of needles; and we cannot tell if a needle or group is dangerous until it is at least partially assembled. So, in principle at least, we must track all the needle pieces all of the time and consider all possible combinations. (Bamford, 2008, p. 102)

John Poindexter was the driving force behind Total Information Awareness (TIA), the program started under the aegis of the Department of Defense. Poindexter graduated at the top of his class at the Naval Academy, but was also the highest ranking official to be found guilty as a result of his role in the Iran-Contra scandal (Bamford, 2008). TIA was the method the government was going to use to track

the needles and try to assemble all of the combinations that the needle pieces could make.

Most of the literature which advances surveillance as a solution to terrorism and/or defends the practice of surveillance advances (or defends) the thesis that increased surveillance decreases terrorism and or crime. This thesis is advanced without a foundational argument; the assertion is made as an article of faith. It is argued that surveillance as a preventive measure is a postulate that needs no explanation. Evidence is proffered for the practical effects of surveillance, (*Report from the field*, 2004), and other statements are made to the effect that the surveillance works, but the public cannot be told the manner in which it works (Levey, 2006) because to do so would compromise the effect of it working.

The theory of surveillance as a tool to prevent terrorism appears to have two components. The first component involves finding and tracking known terrorists. Once a terrorist is found, the tracking is not stopped nor the terrorist apprehended. The next phase involves finding the wider web of relationships of which the terrorist is part. The web of investigation grows, and the people associated with the initial individual being investigated, are themselves investigated, and then their associates.

Of course, there is the argument that, this being the case, bin Laden should have been caught by now (Devita-Raeburn, 2008). Devita-Raeburn examined Milgram's original small world study (Milgram, 1967). Even though Devita-Raeburn noted weaknesses in the statistical analysis of the study, the popular supposition that these connections are the case is ingrained in the culture. The explanation she arrived at involved questions of socio-economic status and motivation, in that the chains that are not finished due to some connectivity failure, fail to complete because of a lack of motivation. Additionally, the original

Milgram study used and targeted individuals in average to above-average socio-economic classes which tended to have more connections among more strata.

Milgram (1974) was famous for his study of obedience in which experimental subjects were tested to see at what point they would stop administering painful electric shocks to actors posing as experimental subjects. In a shocking reprise of circumstances thought to be similar to those that Nazi camp guards and soldiers would encounter, almost all of the subjects in Milgram's famous experiment were to administer what they believed were fatal doses of electric current. It is useful to bear in mind that in the Milgram study, law-abiding citizens conducted themselves in unlawful ways based on the assurance that what they did was necessary. Thus, when members of the security apparatus in today's society are asked to break the law, such as in the case of warrantless wiretapping activities, or when issuing National Security Letters in violation of FBI guidelines (Jordan, 2007), for the "security of the country," it is easy to understand that they are well-intentioned but misinformed and misguided criminals.

The second component involves monitoring individuals' activities and using the results of this monitoring to predict whether the individual is going to commit a terrorist act. In the immediate circumstance, the individual's behavior would be compared with the behavior of an individual who was going to commit a terrorist act. The baseline for prediction would be developed by monitoring everyone all the time, then when someone commits a terrorist act, the activities of that individual could be replayed up to the point of the launch of the attack. If the behavior of the observed individual matches the behavior of those who have launched terrorist attacks in the past, prior to the launch of the attack, then the individual exhibiting that behavior could be prevented from committing the terrorist attack. This thinking was behind the other purpose of the Total Information Awareness (TIA) program.

There are now only gross approximations of indicators that law enforcement and intelligence community members use to identify potential terrorists (leaving out the rhetorical question of who would not be a “potential terrorist”), and some of these are bad for journalists. For instance, according to the current law enforcement manuals, the use of cameras and video equipment is considered a precursor to terrorism (Goodman, Rosa, German, & Clancy, 2008).

It is instructive to understand the rationale of the surveillance advocates and attempt to find the reasons behind society’s redefinition of the right of privacy. The rhetoric of surveillance proponents is a good place to start and can be examined in the context of post 9/11 legal and policy initiatives, although there had been significant work in the surveillance arena prior to the attacks of 9/11. This rhetoric must be examined in the light of the terrorist threat which underpins the reasons that citizens seem unconcerned for their liberty and trust the government to use the powers it has gained by circumventing the Constitution to society’s benefit.

## 2.1. What is Terrorism?

Various government agencies and recognized experts in the field of terrorism have constructed and apply differing definitions of the term “terrorism.” In popular discourse, unpopular individuals and causes are labeled terrorists (Pabst, 2006). The term as used in the press is amorphous and is commonly misapplied by the media and government interests (Pumphrey, 2003). Before September 11, 2001, however, there were attempts to define terrorism in ways in which scholars could agree.

These serious attempts in the field of terrorism studies to define the term terrorism have led to various degrees of precision in defining the term. Badey (1999) attempts to define terrorism while noting that “there is still no commonly

accepted definition of international terrorism" (p.90). Badey refers to work by Alex P. Schmid, attempting to craft a definition of terrorism as a synthesis of 109 definitions. The result was a very precise, yet very verbose definition. Badey contrasts the Schmid definition with the 1983 definition contained in Title 22 of the United States Code, Section 2656(d), which is shorter, yet more general. Badey correctly notes that governments define terrorism in ways that allow them maximum flexibility in characterizing politically significant events in terms advantageous to the government describing them.

Pragmatically, due to the multi-national nature of terrorism, it seems as if it would be important for states to agree on the definition of terrorism in order to cooperate in the suppression of terrorism, although states are generally in agreement with what constitutes terrorism in times of peace. The definition has evolved in the rubric of "customary law" over time (Cassese, 2006, p. 933). However, in other circumstances, such as in terms of armed resistance to an occupation, there is less agreement. There is an element of one political or policy interest group's "terrorist" as another's "freedom fighter." Under international law, there are distinctions between violations regarding civilian populations for states – such that states can rarely be held accountable for "state-sponsored terrorism" (Cassese, 2006). The key is for the state to kill (or at least attack) an "enemy combatant" and keep the incidence of civilian deaths (collateral damage) from being "disproportionate." The big disagreement is what to do with "freedom fighters" who are fighting to end an occupation, and what their culpability is in the case of civilian casualties. In almost every case, it is agreed that non-state actors killing civilians are guilty of terrorism, while killing civilians in an armed conflict could, in the worst case for the aggressor, raise the offense to only the status of "war crime" (Cassese, 2006, p. 946).

Hoffman (1998) also looked at 109 definitions of terrorism and calculated the frequencies of certain conceptual elements, including violence, that terrorism is

political, emphasis on fear etc. Broad variations in frequency were found, with (only) 83.5% of the definitions including violence or force conceptually, to the idea of demands being made on third parties included in only four percent of the definitions (Hoffman, 1998, p. 40). Thus there is a wide variation in the intersection of definitional elements, allowing for rhetors to manipulate the meaning of what is considered to be terrorism merely using the construction of the definition of terrorism.

The term terror entered the lexicon originating from a description of state action during the French Revolution. The *terrors* were a tool of the state to enforce compliance and order during the period of turmoil following the uprisings of 1789, specifically the French government's actions against their domestic enemies in 1793 and 1794 (Tilly, 2004). Therefore, the use of the term terror in a political context in the modern day is well-divorced from the manner of use of the term from the time of the French Revolution.

Terrorism, according to the United States Department of State in 1983, was explicitly described as political and a tool used by non-state actors or "clandestine agents." This was the manner in which modern international terrorism was presented in the popular discourse prior to 9/11. Acts of terror in definitions of terrorism are designed to induce fear which would influence behavior. Many definitions are concerned with the repeatability of acts of terror, in that if an act in itself is an isolated act of terror which has no possibility of being repeated, is it terrorism under the definition? (Badey, 1998) In the popular discourse, the Oklahoma City bombing, even though it had no possibility of being repeatable (by the same perpetrator(s) or organization, as the government said there was no organization), is referred to as terrorism (Lewis, 2000).

Historically, modern terror's origins can be traced to the Narodnaya Volva (People's Will) in czarist Russia. The group was founded in 1878 with the

purpose of committing dramatic acts of violence to awaken the apathetic Russian people and rally them to the anti-czarist cause. There was a successful assassination, that of Czar Alexander II in 1881.

Operationally, the chain of events following the assassination led to anarchists and anti-government revolutionaries discovering the concept of organizing into small “cells,” or groups of individuals. This organization into cells served the purposes of avoiding detection by police and minimizing the amount of damage to which discovery could lead if one of the members were to be discovered and confess their anti-government associations (Hoffman, 1998).

Anarchists were responsible for several political assassinations, including the assassination of Archduke Franz Ferdinand in Sarajevo in 1914. Despite their success in killing heads of state and politically important personages, those events did not have the effects desired by the revolutionists. Political life and power structures were not changed by these events.

Anarchists were described as such during that time, although their actions could arguably fit into the definition of terrorism. Their actions were repeatable, in that they were attempting to build an international fellowship of anarchists. Their aim was to affect behavior, hoping to affect political change in all spheres of political and societal structure. Their actions were intended to affect the target group, in this case individuals in power, and there was a certain amount of fear that they hoped to inspire in the target groups (Hoffman, 1998). Thus, anarchists could be considered ideologically motivated terrorists.

States are also known to sponsor terrorists for their political ends. These terrorists are known as “state-sponsored terrorists.” These terrorists are considered to be even more dangerous than terrorists who must raise their own money. State-sponsored terrorists have access to money and expertise to which

they would not otherwise have access. The danger that state-sponsored terrorists pose to their “constituents” is that state-sponsored terrorists also have latitude to conduct operations that they might not have contemplated were they not sponsored; operations which might cause collateral damage among their perceived constituents, due to the disconnect between their funding sources and the actual population they are ostensibly representing (Jenkins, 1986).

The destructive capability of terrorist groups at all times throughout history was limited by the capabilities of the weapons they could bring under their control. These weapons, by definition, were the most deadly weapons for which the technology existed at the time. Prior to the advent of gunpowder, terrorists would have had to use knives and swords. With gunpowder, there was the ability to make bombs. Until the advent of weapons of mass destruction, the best terrorists could do was to use explosives. However, with the advent of chemical, biological and nuclear weapons came the ability to cause damage on a much greater scale (Laqueur, 1999).

These more powerful and more destructive weapons also require a will to use them. Laqueur (1999) describes the “New Terrorism,” which involves terrorists who have the will to use weapons of great destructive power. The motivations of these terrorists may not be traditional in the sense that they are not working toward what would be considered politically achievable aims. The motivations that these terrorists possess are expected to be extreme, and possibly the most dangerous and extreme position is that of religious fanaticism.

## 2.2. The Terrorist Threat

The United States government asserts that the reason the government is compelled to conduct surveillance on its citizens is that the government must protect the citizens of the country from terrorism. The claim is that surveillance is

necessary to discover and pre-empt terrorists. The seminal event which the government points to in generating consensus for its surveillance activities is the attack by “international terrorists” of September 11, 2001 (Bloss, 2008). Terrorism studies scholars have attempted to rigorously define the meaning of the term “terrorism.” The term terrorism is used differently in popular discourse than the manner in which scholars use the term. This observation is included due to the fact that it is the popular definition which is used as the touchstone upon which policy decisions are made by the government and consensus is obtained for those decisions (Badey, 1998; “USA PATRIOT Act,” 2001).

It is accepted as fact that 19 men, 15 individuals traceable to Saudi Arabia, two individuals from the United Arab Emirates, one from Egypt and one from Lebanon were involved in the hijackings and subsequent crashing of airplanes into the World Trade Center and the Pentagon on September 11, 2001 (Johnston, 2003). These terrorists acted under orders of al Qaeda leader Osama bin Laden, whose organization took credit for the attacks. Department of Homeland Security Michael Chertoff refers to the attacks of 9/11 as a defining moment in U.S. history (Chertoff, 2006a).

September of 2001 was not, however, the first time that the World Trade Center had been attacked by terrorists. A truck with a bomb in it had been driven into the parking garage in 1993 and detonated, leaving six dead and over 1,000 wounded ("Significant terrorist incidents," 2004). Similarly, according to the State Department, the bombing in Oklahoma City, a single incident attributed to Terry Nichols and Timothy McVeigh, is considered terrorism ("Significant terrorist incidents," 2004). Although the Oklahoma City bombing lacked repeatability, which most scholarship considers to be a litmus test in the definition of terror (Badey, 1998; Hoffman, 1998), under USA PATRIOT Act, passed in October 2001, the Oklahoma City bombing is definitely considered to be terrorism. Under

many definitions of terrorism, a pattern of lighting churches on fire or bombing abortion clinics could be considered domestic terrorism.

The USA PATRIOT Act in Section 802 expanded the definition of domestic terrorism for criminal consideration to include ‘‘…activities that— (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended— (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States” ("USA PATRIOT Act," 2001). This would fit the Oklahoma City bombings squarely within the rubric of terrorism if it was not considered so under previous law.

## 2.3. Pre-empting Terrorists

There are several components to the art or science of preventing terrorism. Identification of terrorists would be the first issue. Intuitively, the first thought would be to identify and apprehend those who have committed terrorist acts in the past, and punish them.

However, according to prevailing anti-terrorism theory, the operational construct involves observing and monitoring the terrorists to allow the known terrorists to lead investigators to additional unknown terrorists. The theory in this case involves the supposition that those who may have committed terrorist acts in the past would associate with those who would commit terrorist acts in the future with a higher probability and frequency than the average United States citizen.

The 9/11 Commission investigated the sequence of events that led to the attacks on September 11, 2001. Commission investigators pieced together a picture of

who knew what, when. The 9/11 report indicates that the government had knowledge of the identities and whereabouts of key terrorists involved in the 9/11 hijackings, and despite ample warning that these individuals were in the United States, did nothing to stop them (9/11 Commission, 2004). Additionally and after the fact, Bamford (2008), in interviews conducted at NSA, discovered that no 9/11 Commission members interviewed anyone from NSA to see what was known at that agency. It turns out that NSA knew the terrorists were interesting targets and was listening in on the 9/11 hijackers for months before the attacks. NSA passed the information to CIA and the information was then not forwarded to the FBI for investigation. In any event, it is accepted there were key failures in the handoff of information regarding these terrorists (9/11 Commission, 2004). This highlights a key problem in the growing surveillance society: there is so much information potentially and actually available that interagency communication and prioritization is nearly impossible. In other words, security agencies suffer from information overload.

Two of the hijackers, Nawaf al-Hazni and Khalid al-Mihdhar, were known to the U.S. intelligence community for their involvement with the 1998 embassy bombings in Tanzania and Kenya. These bombings had been the work of al-Qaeda, and these two were implicated. In January 2000, it was discovered that these two individuals were in attendance at a secret terrorist planning meeting in Kuala Lumpur. In March 2000, the CIA had been informed of the fact that al-Hazmi flew to Los Angeles from Malaysia on United Airlines. The CIA failed to notify any agency which could have stopped or monitored al-Hazmi. Denying entry to the U.S., arrest or surveillance against al-Hazmi was possible under the laws as they existed at the time (Jonas & Harper, 2006).

NSA director General Mike Hayden had been worried about getting the NSA in trouble for breaking the law, as the agency had in the past. Therefore, the director, even though his agency had been intercepting those known terrorists'

communication, did not divulge information gleaned from the surveillance. General Hayden, in an excess of caution to avoid having NSA officials accused of breaking the law, as they had in the past, stopped monitoring all calls involving any person in the U.S., including calls of suspected terrorists (Bamford, 2008, p. 27).

However, before the meeting in Kuala Lumpur, the NSA had intercepted a call to Khalid al-Mindhar in late December 1999. This call was intercepted, terminating at a house in Yemen the intelligence community knew al-Qaeda was using as an operations center. It had been used in planning the operation against the *U.S.S. Cole* and identified as such in the investigation into the attack on the *Cole*. The NSA only picked up first names in the call indicating that the terrorists would be meeting in Kuala Lumpur. The failure by the NSA to look up the names Khalid and Nawaf was the first of many oversights committed by the intelligence community. In the case of this first NSA misstep, it is reported that the NSA was deliberately doing as little as possible in identifying the subjects of their investigation because of professional rivalries with the CIA (Bamford, 2008, p. 17).

If the goal of surveillance is as the government says it is, anti-terrorism and the identification of terrorists, this situation would be remedied with the new powers the government has granted itself. However, the logical conclusion is that the surveillance regime, as it was constituted before the current push for ubiquitous surveillance, if correctly applied, would have resulted in the apprehension of the individuals who posed a threat to the United States. The government had all the information it needed to prevent the attacks of 9/11 with the intelligence apparatus it possessed at the time. The question, then, is what is to be gained by new incursions against individual privacy—certainly much stands to be lost.

Another component involves the idea that once these terrorists are identified, their associates could also be identified, on the theory that individuals with which the terrorists are in communication would be individuals who might pose a risk to the United States. In this case, terrorists would be identified, surveilled, and then their associates would be identified and surveilled.

A corollary to this theory involves the placement of these individuals' names on various lists. Some of the lists include the No-Fly List and the Terrorist Watch List (Goodman et al., 2008). The theory in this case holds that a terrorist might not know he/she has been identified as a terrorist, and would attempt to board a plane or enter through a border checkpoint, use a real name, and be apprehended. Thus far, unfortunately for the proponents of this theory, there have been no known instances of a terrorist being apprehended in this manner. There are many instances, however, of people who have been delayed in their attempts to fly. Some of these include Catherine Stevens, wife of Senator Ted Stevens (R-Alaska) and Senator Ted Kennedy (D-Massachusetts). In Catherine Stevens' case, her name is similar to the name of a formerly popular rock and roll singer whose stage name was Cat Stevens but who now goes by the name of Yusuf Islam. Ted Kennedy has been repeatedly delayed because there is an Irish terrorist who goes by that name (Marek, 2007). The theory's proponents hope that at some point a terrorist will fall into the No-Fly List trap that the government has set.

Alternatively, the government might actually keep the list as a mechanism to scare terrorists away from airplanes. This would tend to keep them from being able to travel freely in the U.S., tripping tracking mechanisms when they show up at airports. This also assumes that with all of the new surveillance powers the government has that somehow the terrorists are lost in the shuffle until they show up at the airport, thus alerting the government as to their whereabouts.

The most overarching view of terrorism, its prevention, and the surveillance necessary to achieve this preventative stance can be found in the rhetoric of the government's political appointees who are responsible for evangelizing for the need for total surveillance. Part of this surveillance involves the warrantless wiretapping program and other data collection efforts by the NSA (Gorman, 2008).

John Yoo has been responsible for some of the current thought on the manner in which terrorists can be preempted. In his explanation for the reasons that the President has the authorization to order surveillance without having to follow procedures that would normally have to be followed under FISA, the operational advantages of the surveillance are extolled. General Hayden, director of the NSA during the warrantless wiretapping program, said that the program had been successful in detecting and preventing attacks in the United States. Attorney General Alberto Gonzalez also stated that the programs had been effective (Yoo, 2006, p. 104).

According to current U.S. government thinking, the most dangerous terrorist organization is al Qaeda. Al Qaeda was responsible for 9/11, the attack on the *U.S.S. Cole*, and bombings at two embassies in Africa, among other attacks. Therefore, the government is very concerned with members of al Qaeda's movements and intentions.

## 2.4. Religious Extremists and Their Effect on Geopolitics

Al Qaeda is an organization of terrorists with the stated goal of attacking the West. These terrorists are motivated by religion as an ideology. The terrorists who are members of this organization are also fanatics to the point of being able

to commit suicide in the course of their terrorism, which is what happened when the terrorists attacked on 9/11/2001 (Doran, 2002).

On September 11, 2001, the terrorists hijacked four airplanes. United Airlines Flight 175 struck the South Tower of the World Trade Center. American Flight 11 crashed into the North Tower of the World Trade Center. American Airlines Flight 77 flew into the Pentagon. United Flight 93 did not make it to its intended target. The passengers, having been alerted to the other hijacking events, overpowered the hijackers and the plane crashed into a field in Pennsylvania. It was speculated that United 93 was heading toward the Capitol or the White House (9/11 commission, 2004).

The latest official count of the people who died in the World Trade Center on 9/11 is 2751. The total number of people who died in the attacks that day was 2975 ("Official 9/11 death toll," 2008), and the American public was horrified.

Prior to the attacks of September 11, al-Qaeda had attacked several other Western targets with varying degrees of success. In August 1998, two American embassies were bombed simultaneously. At the embassy in Nairobi, Kenya, the bombing killed 12 Americans, 32 other United States employees, and over 200 Kenyans. In Dar es Salaam, Tanzania, no Americans were killed, however 11 individuals were killed and 85 injured (Crenshaw, 2001). In October 2000, the U.S.S. Cole was attacked by a boat retrofitted as a bomb, 17 American servicemen were killed, and 39 were injured (Abdul-Alim, 2000).

Al Qaeda was a powerful terrorist network, capable of international terrorism on a scale that was of concern to the United States. After the embassy bombings, the United States retaliated with cruise missile strikes against al Qaeda training camps in Afghanistan, and a pharmaceutical plant in Sudan (Crenshaw, 2001).

Al-Qaeda has a pre-history which is often conveniently overlooked. This has to do with the fact that starting with the Carter administration, agencies of the United States government gave financial support and arms to the mujahedeen to fight the Soviet Union in Afghanistan (Schneider & Schneider, 2002).

There is some disagreement over the structure of al Qaeda, whether it is a coherent international terror organization, or merely a loose, informal affiliation of like-minded terrorist operatives (Burke, 2004). Mr. Gunaratna in hearings before a United States Congressional committee stated that al Qaeda was organized according to a charter published in Al Jihad, a publication printed in Peshawar, Pakistan, in March 1988 (*Terrorism, Al Qaeda*, 2003). Mr. Gunaratna quotes the publication as claiming that "al Qaeda is the vanguard, 'the pioneering vanguard of the Islamic movements.'" This vanguard, according to Mr. Gunaratna, would inspire other Islamic movements to also attack Western interests.

This manifesto was attributed to Dr. Abdullah Azzam. Burke (2004) quotes Dr. Azzam as calling in 1987 for *al-qaeda al-sulbah*, "a vanguard of the strong." These are identical quotations, but are interpreted differently by the two scholars. Burke makes the assertion that the term "al Qaeda" was coined after the 1998 U.S. Embassy bombings in East Africa, in order that American laws could be applied to the perpetrators of those bombings. Burke explains that in 2004, Israeli intelligence services would refer to the Muslim extremists as "jihadi international" instead of "al Qaeda" for the reason that Israeli intelligence considered the jihadi movement to be decentralized and not to have coherent leadership (Burke, 2004).

The amorphous nature of the terminological and definitional semantics makes President Bush's discussion of "al Qaeda in Iraq" either logical or disingenuous, depending on the viewpoint of the receiver of the rhetoric of identification.

Due to the fact that al Qaeda is a distributed organization, with semi-autonomous operational units, the order of priorities of the aims of al-Qaeda likewise is not necessarily coherent.

Marc Sageman explained to Congress that bin Laden has been crucial in operationally defining the direction and subject of the attacks of these affiliated groups. It was bin Laden's fatwa in 1996 which changed the focus from the "near enemy" to the "far enemy." This involves the concept of corrupted states. As an example, Muslim extremists had been at war with their own government in Egypt. The government of Egypt was considered to be jahiliyya. Jahiliyya refers to the barbaric state of ignorance which existed before the prophet's revelations. Once the prophet imparted the knowledge contained in the Quran, Islamic states would need to, according to the Salafists, impose Sharia law to be a proper Muslim state (*Terrorism, Al Qaeda*, 2003).

The 9/11 discussion had as its initial focus the terror network headed by Osama Bin Laden. Yet, it was with the help of the Taliban that bin Laden's network was able to flourish and train (*Terrorism, Al Qaeda*, 2003).

Mamoun Fandy, testifying before the same committee, made the observation that there were other Islamic terror groups which were coordinating with each other to carry out attacks internationally. The attacks occurred over a wide swath of territories, with multiple countries of origin.

In some scholarly efforts to try to understand the structure and characteristics of terrorist organizations, comparisons have been made between al Qaeda and the Sicilian mafia and pirates of the 17th century. Structurally and functionally, these organizations are similar, even if their motivations are not. For instance they:

> …have some attributes in common: their cellular and networked structures extending across national boundaries; their high levels of energy, fed by sentiments of revenge; their sponsorship by states or elements of states; their parasitic revenue streams from

> licit and illicit commerce, and their tendency toward extraordinary violence in some historical moments, provoking a determined, and generally publicly supported, "crackdown." (Schneider & Schneider, 2002, p. 776).

This would then be a hook for the counter-terrorists to take a page out of the enforcement efforts used against the mafia. The use of the organizational structure against organizations such as these would entail the types of signals intelligence at which the United States is proficient, in the form of intercepted communications, wiretaps and surveillance. Additionally, in mafia cases there would always seem to have been an informant of some type, or some testimony on the inside. In the case of the al-Qaeda, there wouldn't seem to be much need for testimony, just locational and organizational information as assassination is the preferred method of justice.

Other scholarship involves an attempt to ascribe and understand some type of root cause for Islamic terrorism. One of the common themes has to do with the concerns of anti-globalist sentiment. Market capitalism has transformed the world. The organization of transactions based on market capitalism is that the transactions are based on contracts. Economic historians have identified two main types of exchange, those based on markets and clientalist exchange.

Markets and market forces are well known to Westerners, as that is the economic system to which the United States and the global trading community adhere. Clientalist structures are mostly recognized as tribal or clan-centric. The members of the community are clients of the tribal leader or head of the clan. These structures manifest themselves as kingdoms or caliphates at the nation-state level of organization, and thus are thought by Western standards to be almost medieval or feudal in nature.

There is a difference in organization of the communities based on these types of systems, wherein clientalist communities are hierarchically organized. All societies have some combination of market and clientalistic characteristics,

however the liberal democracies have advanced market-based economies, and few states have predominantly clientalist economies, so this fact might be a key difference in the cultural differences which might lead to the feelings of ill-will.

As Mousseau (2002)/2003) notes, the in-groups in clientalist societies with mineral wealth can spread that wealth around to maintain and gain more loyalty and to keep power. For societies without mineral wealth, underdevelopment and economic displacement results in increasing the social and civil ills. The market economy appears to be a Western or American invention and therefore the resentment inherent in the society at the economic and social ills is projected on the Western market system and the West in general (Mousseau, 2002/2003, p. 17).

The United States government is focused on the language of war in the discussion of the “Global War on Terror.” From a counter-terrorism perspective it is this rhetoric of war and concern for operational security which makes U.S. intelligence services obsessed with signals intelligence.

## 2.5. Technologies of Surveillance

The type and amount of surveillance an individual may be subject to on a daily basis varies depending on the types of activities in which the individual engages. The presence of technologies of surveillance, insofar as these technologies are used in daily life, has been introduced previously. These technologies include Internet and email surveillance, telephone and cell phone surveillance, and the surveillance engendered by optical monitoring of public spaces. These types of monitoring and surveillance are relatively mundane and need little explanation.

Additionally, the technologies can be divided into content-based and location-based monitoring. That is, the Internet and phones (used only as phones and not

as a locational beacon) are of little use for monitoring an individual without the content which is transmitted across the network. If someone is moving around and not talking on the phone or using the Internet, how would those conducting the surveillance know where the individual might be?

The technology of location is demonstrated by the location-assisting technology in cell phones and the monitoring that cameras provide. These technologies present slight problems in the ease of tracking. Not everyone has a cell phone. For those who do, even though cell phone tracking takes a fair amount of processing power for triangulation, the exercise of tracking that individual, and all individuals with cell phones, is trivial. As of 2006, those who do have cell phones generally keep their cell phones on or about their persons ("The cell phone challenge," 2006), so tracking them using these beacons is a simple matter.

For good results in tracking individuals, those doing the tracking need some type of mechanism such that every individual has some type of beacon. Ubiquitous RFID tracking fulfills that need. Anything can be tagged and tracked, even by a home user (Cangeloso, 2008).

The most unobtrusive tracking technology, and easiest to use for tracking any manner of object, is the RFID tag. Advances in technology have produced RFID tags which can be as small as a grain of sand, and therefore can be embedded in almost any item. The component which renders the discovery of RFID tags unobtrusive is the fact that there is no way for the average individual to know that a reader was scanning all of the RFID tags embedded in the items they were wearing or carrying (Fishkin, Jiang, Philipose, & Roy, 2004).

Proponents of RFID espouse a vision of the future in which every discrete item is tagged. Every aspirin bottle, every shoe, every tire, every car, every belt and every pair of jeans would have an RFID chip embedded. Every pair of

eyeglasses, purse, backpack, book, pen, pencil, pencil sharpener, package of gum or breath mints; all of these would be tagged. In this future, when an individual walks into a retail establishment, the readers at the doorway would enable the sales staff to know every item that is in an individual's wallet, every item they were wearing and every item they were carrying. With proper data integration, the salesman at the clothes store could tell the customer that his socks were bought several years ago and would the customer like some socks with their purchase ("RFID, a vision," 2007).

Under the provisions of law regarding data collection and sharing, every encounter with the reader could be written to a national security database and not be illegal under the privacy laws as they stand now. No change to the law would be required in this eventuality. This would allow the trail of a person shopping at the mall, for instance, to be followed, in real time if necessary. In this way, the government would be able to track every person, and know, for instance, if a person stopped into a book store, did or did not buy something and then went to the military surplus store. The few minutes spent looking at the latest gadgets at Radio Shack would be noted, as well as the stop at the information kiosk asking for directions to a certain other store.

With advancements in the technology, there could be readers at multiple locations in stores. These arrays of multiple readers would allow those who were watching to know near which products the consumer stopped or loitered. According to experiments which were conducted by IBM in Germany, the watchers would know what products were more interesting to consumers, by combining the RFID tracking with feeds from CCTVs ("German consumers," 2004). The idea is to determine the time a consumer spends looking at some item by combining the feed from the RFID readers with some other surveillance technologies to help the retailers ("METRO Group," 2003).

Sometimes, the surveillance works but is not effectively coordinated with the agencies that need to receive and act on the information. An example of this might be when the United States Agency for International Development gives U.S. taxpayer money to individuals and groups tied to terrorists. For instance, USAID gave $1 million to an individual who lied to federal agents about his ties to a disciple of bin Laden, and $180,000 to a Bosnian group whose president is on a watch list and is barred from entering the United States (Tankersley, 2007).

# CHAPTER 3. TOTAL SURVEILLANCE FOR SECURITY - ASSUMPTIONS

## 3.1. Counter-Terrorism

The reason given to the American people for the imposition of dramatic new surveillance measures and the limitation of individuals' rights under the law was the need to fight terrorism. The fundamental assumption is that there is not just a way to discover known and active terrorists through surveillance, but also a way to predict who might become a terrorist and how or when terrorist acts might be committed.

There are two components inherent in the problem of counter-terrorism. The first is to identify terrorists. The second is the question of what to do with the terrorists once they've been identified.

The problem of identifying terrorists can itself be broken down into two components. The first component is the identification of those who have committed terrorist acts in the past. It can further be assumed that those who have committed terrorist acts in the past would be plotting to commit terrorist acts in the future. The second component has to do with attempting to identify terrorists before they become terrorists. This is the predictive aspect of the policy of prevention of terrorism.

The 1978 Foreign Intelligence and Surveillance Act specified the manner in which eavesdropping warrants were to be obtained for the purposes of conducting surveillance against suspected agents of foreign powers and suspected terrorists. In the aftermath of 9/11, members of the Bush

administration claimed that FISA hamstrung the ability of law enforcement and intelligence services to conduct surveillance. The reason for the surveillance the government wanted to conduct was for the purpose of “preventing” terrorism. Preventing terrorism became a top priority of the administration, and five years after 9/11, the Executive Branch published the updated *National Strategy for Combating Terrorism*. The original national strategy document was published in February 2003. This document outlines the steps that the U.S. government would take to combat terrorism (National strategy, 2006).

The White House has published more over-arching guidelines which integrate and discuss the strategies in the *National Strategy to Combat Terrorist Travel, National Strategy for Maritime Travel*, and *National Strategy for Aviation Security*. The elements of the strategies that insinuate themselves into a discussion of privacy and surveillance have to do with the identity intiatives, and law enforcement and intelligence gathering initiatives.

In the rhetoric surrounding the White House initiative to prevent and disrupt terrorist attacks, the Executive Branch states that the U.S. “law enforcement and intelligence communities must have detailed knowledge of our Homeland adversaries, including their identities, sources of support, intentions, capabilities and modi operandi” ("Prevent and disrupt," 2007, par. 11). After discussion of collaboration without specifying collaboration between which entities, further explanation leads to a desire to promote the “implementation of Intelligence-Led Policing by State, local, and Tribal law enforcement – after all, they best understand their communities, citizens, and current trend lines” ("Prevent and disrupt," 2007, par. 12).

Another strategy for counter-terrorist purposes has to do with tracking money as it moves around internationally. The United States has been successful in applying the PATRIOT Act and other laws which track banking activity, transfer of

moneys and international banking transactions in cases in which the organizations host information in the U.S.

The Society for Worldwide Interbank Financial Transactions (SWIFT) was one such entity. However, the payments processing body announced that it would stop processing European banking transactions in the U.S. in 2009 after criticism from E.U. data protection officials. SWIFT officials said they had to turn over data on European citizens' banking transfers because the data was stored in the U.S. In 2009, E.U.-U.S. transactions would still be hosted in the U.S., and therefore subject to counter-terrorist surveillance, but a new processing center in Switzerland would handle intra-European payment processing ("SWIFT to stop," 2007).

Another strategy that counter-terrorism experts promote is the idea of predictive data mining, much as the example of the partially assembled needles. This another example of a strategy that is given and taken on faith, as the problem with predicting terrorism is it is a problem with indeterminate boundaries in which data analysts have little experience. Even in commercial applications, data mining produces an unacceptable percentage of false positives. The example given by Jonas and Harper (2006) is what life would be like if a false positive rate of 1% or even 0.1% were realized (1% and 0.1% are orders of magnitude smaller than real percentages of false positives from commercial data mining). In a population of 300,000,000, the FBI would have to investigate 3,000,000 or 300,000 individuals (Jonas & Harper, 2006, p. 8).

### 3.2. Putting the Local Populace Under Surveillance

This line of reasoning leads to the recommendation that: "the Federal Government will recommend priorities for State, local and Tribal homeland security activities that focus resources on the most pressing problems, adopt a

formal intelligence process with requirements generation and tasking of information collection, and analyze and disseminate the information" ("Prevent and disrupt," 2007, p. par. 12). In line with this statement of philosophy, the Federal Government will direct state and local law enforcement in their intelligence collection efforts throughout the Homeland.

There is a critical issue that needs to be addressed in the domestic intelligence community, and that is the criteria used in the development of tasks for local law enforcement in terms of intelligence gathering. How will information be developed? What information will trigger an investigation? The current set of guiding principles can be discerned from the following:

> In order to uncover terrorists and terrorist activity against the backdrop of our highly mobile, dynamic, and diverse society, we must attain domain awareness of the actions, events, and trends that occur throughout our land, maritime, air, space and cyber domains. This is a multi-faceted process. First, partners throughout the entire law enforcement community must continue to enhance their baseline understanding of their operating environments – the people, the geography, and the daily and weekly rhythm of activities and events. By understanding trend lines, we can better identify anomalies and deviations that could indicate terrorist activity. ("Prevent and disrupt," 2007, p. par. 11)

The people they are referencing in the document are United States citizens. The "anomalies and deviations" could be such actions as political protest or groups meeting to discuss how to effect policy change, i.e., legitimate political dissent, as the following example illustrates.

"Undercover Maryland State Police officers repeatedly spied on peace activists and anti-death penalty groups…" (Madigan, 2008, par. 1). 43 pages of documents, much of it redacted, obtained by the ACLU describing the infiltration of non-violent groups whose aim was to effect policy change of their government, even though there was no evidence of criminal or potentially criminal acts. The Maryland State Police conducted surveillance, so far as was discovered, for at least 288 hours over 14 months in 2005 and 2006.

One individual who had drawn government scrutiny was Max Obuszewski. His name is currently in the Washington/Baltimore High Intensity Drug Trafficking Area database.

David Rocah, an ACLU attorney, said, “Everything in these logs is a lawful First Amendment Activity. For undercover police officers to spend hundreds of hours entering information about lawful political protest activities into a criminal database is an unconscionable waste of taxpayer dollars and does nothing to make is safer from actual terrorists or drug dealers…(Madigan, 2008, par. 6). Mr. Obuszewski has devoted his entire life to peace. If there is anyone in the world who is further from a terrorist it is hard for me to imagine” (Madigan, 2008, par. 18).

An ACLU policy counsel, Michael German, who is a former FBI agent and who at the FBI was an expert in counter-terrorism, said, “It serves no security purpose to infiltrate peaceful groups. It completely misuses law enforcement resources” (Madigan, 2008, par. 22). Mr. German said that the government has “actively encouraged” local police to gather intelligence and compile information that has no apparent connection to crime.

Mr. Obuszewski seemed puzzled as to the infiltration, explaining that the groups to which he belongs have open meetings and the schedules are publicized. “Why would someone come to those meetings and pretend to be someone else? Why are government agencies targeting pacifists?” he asked (Madigan, 2008, par. 19).

The answer might lie in details of Pentagon surveillance of anti-war groups. NBC News reported that the Department of Defense was collecting information on anti-war protest groups as “potential terrorist threats” (Myers, Pasternak, & Gardella, 2005, p.2)

The names of the people who participated in meetings were shared with at least seven databases, including the NSA, police departments of Baltimore, Baltimore County, Annapolis and Anne Arundel County, and the state General Services police. The information shared with these agencies and departments were such "terrorist-related" activities as setting up a meeting with then-Representative Benjamin Cardin in 2005 to ask him to support a timetable for withdrawal in Iraq. Other information that is stored on these individuals includes, according to Susan Goering, executive director of the ACLU of Maryland in a letter to Governor Martin O'Malley, "…extensive information about specific individuals and groups, including describing their political outlook, and whether they were articulate, [and] what political activities they are engaged in…" (Madigan, 2008, par. 27)

The information was developed as a result of the state police's Homeland Security and Intelligence Division infiltrating the Baltimore Pledge of Resistance, a peace group, the Committee to Save Vernon Evans, who sits on death row, and the Baltimore Coalition Against the Death Penalty. The fact that the state police has a Homeland Security and Intelligence Division and is infiltrating protest groups is evidence of the seriousness with which local and state law enforcement are taking their domestic intelligence imperatives.

The state police maintain that they did nothing illegal and they did not curtail protesters' freedoms. Colonel Terrence B. Sheridan, superintendent of the Maryland State Police, went on to say, "Only when information regarding criminal activity is alleged will police continue to investigate leads to ensure the public safety" (Madigan, 2008, par. 9).

The endgame in this type of surveillance is already appearing in the open elsewhere in the industrialized world. The United States government, as just illustrated, was maintaining a database similar to a database in France maintained by its Defense Department equivalent. The database's name is

Edvige. The charge of those in France setting up and administering the database is to store data on anyone aged 13 or older who is “likely to breach the public order” (Bremmer, 2008, par. 3). The types of individuals whose information is stored in Edvige includes anyone active in politics or trade unions, as well as those with significant roles in business, the media or entertainment, or social or religious institutions.

Herve Morin, the French Defense Minister, publicly breaking with government policy, questioned the usefulness and role of the database, asking, “Is it useful to gather data such as telephone numbers, sexual orientation and details of taxes and assets and so on without knowing exactly what is the point” (Bremmer, 2008, par. 6)?

This illustrates the manner in which governments all over the world are attempting to equate “breaching the public order” with terrorism. This is the same manner in which the United States Criminal Code is currently constructed, as illustrated earlier, in which civil disobedience, which by definition breaches the public order, is equated with “domestic terrorism.” This definition of terrorism may not be the definition with which a civil rights activist in the United States would agree.

The *National Strategy for Combating Terrorism* (2006) describes the endpoint in the war on terrorism in the following terms:

> In the War on Terror, there is also a need for all elements of our Nation – from Federal, State and local governments to the private sector to local communities and individual citizens – to help create and share responsibilities in a Culture of Preparedness. This Culture of Preparedness, which applies to all catastrophes and all hazards, natural or man-made, rests on four principles: a shared acknowledgement of the certainty of future catastrophes and that creating a prepared Nation will be a continuing challenge, the importance of initiative and accountability at all levels of society; the role of citizen and community preparedness; and finally, the roles of each level of government and the private sector in creating a prepared Nation. Built upon a foundation of partnerships, common goals and shared responsibility, the creation of a Culture of Preparedness will be among out most profound and enduring transformations in the broader effort to protect and defend the Homeland. (p. 21)

One of the problems that counter-terrorism operatives face is the problem of individuals who may be terrorists but have not been identified as such. “New recruits, particularly those without criminal records or who are not known to law enforcement, can travel with relative ease from country to country and from city to city with little notice” (Heyman & Carafano, 2008, p. 14). Theoretically, the new powers the government has granted itself will give the counter-terrorists the ability to identify these terrorists who might not have been identified as terrorists without the new powers.

It is not apparent that there is any assumption that the “Global War on Terror” will ever end. In the literature of those who would defend the taking of powers from the people, there is an assumption that the government will return those powers to the people when the crisis has passed. In the history of the United States in which extraordinary powers have been assumed during times of war and national emergency, some of the rights taken from the people were returned, and some of the additional, extraordinary powers assumed by the government were relinquished at the end of the conflict. Even in the case of the Sedition Act of 1918, the law was repealed, although it was passed again (after World War I was over) and remains in effect to this day. What is important to note, however, is the observation that “Unfortunately, history has shown that it is exponentially harder to wrench power away from the government than it is to give it power in the first place” (Branum, 2001).

This particular war may be slightly different, in that there may be no relaxation of the surveillance regime as President Bush declared the war on terror to be “a task that does not end” (Bush, 2001). The sentiment that the war on terror will never end has been echoed by other members of the Bush administration at various times. President Bush’s first national security advisor, in a speech at a U.S. Institute of Peace Conference, compared the war on terror to the war on crime. His sense was that the United States could only win against terrorists "in

the sense that we can win the war on crime. We can break its back so that it is a horrible nuisance and not a paralyzing influence on our societies" (Scowcroft, 2002). The Secretary of Defense at the time of the 9/11 attacks, Donald Rumsfeld, in response to a question of what the endpoint of the war on terror would look like, said, “I think trying to stamp [terrorism] out in every single locale all across the globe in perpetuity sounds like a pretty big task to me” (Rumsfeld, 2001).

Some surveillance activities are decidedly low-tech, and local police are also emboldened by the knowledge that federal laws permit all manner of information gathering in the context of terrorism investigations. In some cases, local police, even if not specifically tasked with gathering information by a federal intelligence agency, attempt to use the federal laws as cover for gathering information not normally available to local police under traditional rules of police investigations. Michele Reutty, a librarian, relates the story of the police attempting to access library records to identify a patron by the book the patron was carrying, who was under investigation for saying something inappropriate to a girl in front of the library.

As the police repeatedly asked for the information on who had checked out which book, Ms. Reutty asked that they follow proper legal procedure and get the proper subpoenas. As the police tried and failed to follow legal procedures, pressure was brought to bear on the librarian. She was threatened with the loss of her job. At a board meeting the powers that be were upset that the story had gotten national attention and that the borough clerk and the police department were getting calls supporting Ms. Reutty’s position that the police get the proper subpoena before she would turn the information over to them. In this particular instance, the incident catapulted her into a new job and provided the impetus for libraries throughout New Jersey to develop a policy for librarians to follow when the police arrive with requests for patron records (Reutty, 2007).

Knowledge of terrorists' and potential terrorists' movements is of use to counter-terrorists and law enforcement, and this type of surveillance is best accomplished with a regime in which individuals can be identified and tracked with some degree of accuracy. The 9/11 Commission recommended that driver's licenses should be more reliable as indicators of individuals' identities (9/11 commission, 2004).

A good link between the identity the individual has on file with the government and the items which are chipped, i.e., have RFID embedded, provides a useful way to track those individuals. Tracking is easier if one of the chipped items is a government issued ID card. An illustration of successes in the Global War on Terror attributed to the new powers the government granted itself comes from a government report. This 2004 report prepared by the U.S. Department of Justice (*Report from the field*, 2004), details the effects the use of the powers granted in the PATRIOT Act had in the disruption and prevention of terrorist attacks, specifically, the case of the "Lackawanna Six."

The Lackawanna Six had traveled to an al-Qaeda camp outside Kandahar in Afghanistan, a Taliban stronghold. According to the Justice Department report, the government was tipped off to the presence of home-grown terrorists by an anonymous letter. The report also made much of the intelligence "wall" that kept law enforcement personnel investigating agents of foreign powers and those investigating common criminals from communicating when the investigation began in the summer of 2001, saying, "…there were times when the intelligence officers and the law enforcement agents concluded that they could not be in the same room during briefings to discuss their respective investigations with each other" (*Report from the field*, 2004, p. 3).

The PATRIOT Act and other laws which followed were desired by the law enforcement and intelligence communities for years prior to the attacks of 9/11.

In May 1995, a report was written for the Attorney General and the Director of Central Intelligence in response to the Banca Nazionale del Lavoro (BNL) and Bank of Credit and Commerce International (BCCI) prosecutions in the early 1990's. The report stated that, "Greater cooperation between law enforcement and intelligence, and better-focused participation by LEA's in proposing intelligence requirements, will lead to better use of existing resources" (*Report to the Attorney General*, 1995, p. 15).

The origin of these problems was the "Wall" memo was written by the Attorney General at the time, Janet Reno, on July 19, 1995 in response to the report. Among the restrictive provisions in the memo concerned contact between a Foreign Intelligence (FI) or Foreign Counter-Intelligence (FCI) Investigation in the circumstance in which no Foreign Intelligence Surveillance Act (FISA) surveillance or searches were being conducted, which stated that, "The FBI shall not contact a U.S. Attorney's Office concerning such an investigation…" (Reno, 1995, Sec. B.2).

With the passage of the PATRIOT Act, the two teams of investigators were able to communicate and the case ended with five of the Six pleading guilty to providing material support to al-Qaeda and the sixth pleading guilty to "conducting transactions unlawfully" with al-Qaeda. The prison sentences were to between seven and ten years for these offenses (*Report from the field*, 2004).

Other successes due to the removal of the "wall" include the cases of the "Portland Seven." In this case, Jeffrey Battle, one of the conspirators, had discussed the terrorist plot he was working on with an undercover informant.

Others in the cell had traveled to Pakistan to take up arms with al-Qaeda against the United States and coalition forces. When they were unsuccessful in their quest, they returned to the United States. The FBI was empowered, through

sections 218 and 504 of the PATRIOT Act, to put these individuals under surveillance while a case was being built, and then capture them before they could commit any terrorism. Six were sent to prison, receiving sentences of three to 18 years each, and the last, Jaber Elbaneh, was killed by Pakistani troops in Pakistan according to the 2004 report. It appears that the report was inaccurate, however, in that the latest news has Jaber Elbaneh at large in Yemen, and on the FBI list of “most wanted terrorists” (Temple-Rastin, 2007a).

Other successes detailed by the government included the successful arrests and/or prosecutions of Sami Al-Arian and co-conspirators in a case of Palestinian Islamic Jihad (PIJ), defendants in the “Virginia Jihad” case, in which the terrorists were associated with an Islamic extremist group known as Lashkar-e-Taiba (LET) and the cases of Mohammed Ali Hasan Al-Moayed and Mohshen Yahya Zayed, both Yemeni citizens, for their involvement with al Qaeda and HAMAS (*Report from the field*, 2004).

Additional successfully prosecuted cases involved racketeers using charities as front groups for support for Chechen rebels, an al Qaeda related drugs-for-weapons plot, and a spying case involving an agent of the former Iraqi government. In all of these cases, the PATRIOT Act was cited as making the difference between success and failure in investigating and prosecuting the cases (*Report from the field*, 2004).

Finally, cases in which the PATRIOT Act has figured prominently involve money transfer and laundering, including cases involving the Columbian rebel group FARC, an arms dealer and operators of unlicensed money transmitting businesses. Additional successes have been achieved in seizing the money and property of terrorists and those with whom they did business. The gist of the report, however, had more to do with the success of tearing down the intelligence/law enforcement “wall,” and stiffer penalties for criminal acts, than

with the successes of surveillance or data-mining initiatives purchasing the government a greater quantity of convictions (*Report from the field*, 2004).

The parallels with anti-terrorism activities in the most surveilled Western democracy, Great Britain, are substantial. The British have the type of camera surveillance build out that that law enforcement in the United States would like to have (Hope, 2008; Temple-Rastin, 2008b). The Fusion Center concept is based on and builds on the Intelligence-Led Policing (ILP) model, which according to Rollins (2008) in his Congressional Research Service report for Congress, "…was gaining favor in the United States following the dramatic drop in crime in Kent, England, where it was originally developed…" (pp. 15-16). Due to the international nature of information sharing among intelligence and law enforcement communities of cooperating countries, initiatives and experiences from Great Britain and the United States cross the Atlantic and therefore create elements of common experience.

The subway bombings in Britain on July 17, 2005 were examples of the importance to the government of surveillance of their citizens. Three bombs exploded in the London subway system at 0720 BST, and one on a bus at 0947, killing 51 innocent people plus the four bombers ("Image," 2005). The Intelligence and Security Committee report released in March, 2006 put the death toll at 52 as one additional injured person died from wounds.

The Prime Minister made a statement on July 11th of that year to say that he knew of "no intelligence specific enough to have allowed then to prevent last Thursday's attacks" (Report into the London, 2006). With this dismissive wave of his hand, the Prime Minister removed emphasis on the question of how the government can prevent terror attacks and why the attacks were not prevented.

The report quotes from a speech by Dame Eliza Manningham-Buller to the Dutch security forces at the Hague, reported in Lord Butler's *Review of Intelligence on Weapons of Mass Destruction (2003-2004)*, as follows:

> The Agencies cannot know everything about everyone, nor can they intercept and read every communication (which in any event would be a gross violation of human rights.) There will always be gaps in the Agencies' knowledge. (p. 7)

The implication is that if the intelligence agencies could intercept and analyze all of everyone's communications, then terrorism could be prevented. The report goes on to discuss the enormous volume of information generated in investigating terrorism, how the U.K. security forces have foiled other plots but didn't foil this one, and the question of the manner in which intelligence is to be prioritized.

One of the bombers was known to have traveled to Pakistan in 2003 and at the time the report was issued, there was no clear connection to international terrorists in terms of external direction and planning (*Report into the London*, 2006, p. 12). It was later established that the bombing was masterminded by Abu Ubaida al-Masri (an alias) of Pakistan and top al-Qaeda leader ("Top Al Qaeda Leader Abu Ubaida al-Masri Confirmed Dead in Pakistan," 2008).

The Security Service had previously had contact with two of the bombers, Siddeque Khan and Shazad Tanweer, the bombers being on the periphery of other investigations (*Report into the London*, 2006, p. 14). Yet the Security Service was absolved of responsibility for supposing to have known to prevent the attacks. The fact that these bombers had been identified from surveillance or terrorist activities and they were not prevented from committing terrorism has had no effect in blunting the force of argument of those who would sell the idea of ubiquitous surveillance as a terrorism prevention solution, regardless of the empirical evidence that the logic may actually be questionable.

London is one of the cities most monitored by closed-circuit TV, and investigators worked for four days going over the camera data from the 3,000 cameras in the London subway system to try to find evidence of the suicide bombers' movements (Milcent & Cai, 2006). After the fact, as illustrated by the rhetoric recounted above, it was not claimed that the surveillance could have prevented the attack. Yet the government calls for more surveillance under a theory advanced by the government that more surveillance could prevent future attacks.

Currently, the British are looking to legalize building a database that will contain all of everyone's communications. The reasons given involve the ability to stop terrorism before it happens (Prince, 2008). The data in the United States already exists, in ISP record retention and phone records, and now with the new FBI guidelines, these are de facto government databases as the FBI can access them with National Security Letters with no judicial oversight, and the FBI needs no probable cause to open an investigation on anyone. Therefore, the data is freely available to the FBI, if it so chooses, for any purpose at any time for any reason (Jordan, 2007; Johnson, 2008).

The question becomes, how much surveillance is enough? Who should be put under surveillance? The answer in the United States is to monitor everyone. Monitoring and tracking everyone is also the answer in Britain. The British are building a huge DNA database, to contain the most personal type of biometric. They have populated it with data from everyone over the age of 10 who has been arrested. This includes those who are not charged, and also includes those who are charged but found innocent. There are now 4.5 million genetic samples in the British DNA database (Townsend & Asthana, 2008). The FBI is also building a massive biometric database (Nakashima, 2007).

There is a call in the United States to install a video surveillance system similar in size and scope to that in Great Britain. On the Fourth of July, 2007, National

Public Radio broadcast a story about American police chiefs who want the type of surveillance power that the British have. There are enough surveillance cameras in Britain, 4,285,000 at last estimate that Scotland Yard can track the movement of every single car in the country from one end of the country to the other (Hope, 2008). Current capabilities allow that the system can store the data for two years.

Miami Police Chief John Timoney used to believe that the surveillance powers a network of cameras that vast represented was too intrusive and that, "…I was opposed to it" (Temple-Rastin, 2007b, par. 6). Not any more. Now he and William Bratton, police chief in Los Angeles, feel these are the tools needed by law enforcement to fight terrorism. There was no mention of the predictive capability that these cameras might give police, but Bratton was impressed with the idea that not just individuals but groups could be identified after the fact as they went places to commit terrorism (Temple-Rastin, 2007b, par. 12).

Civil libertarians are exaggerating the problems with this type of surveillance, Chief Timoney contended. Barry Steinhardt of the ACLU pointed out that the amount of money spent on taking pictures of streets and highways and using those pictures to track people and vehicles would be better spent on investigating and apprehending terrorists. Mr. Steinhardt is also concerned about potential abuses such as tracking innocent people and the police using the camera's abilities for other than its intended purpose, such as "looking for attractive women" as opposed to tracking everyone. But Chief Timoney feels that "most of these concerns have been dealt with." (Temple-Rastin, 2007b)

While it may be true that police have misused the resources at their command for personal purposes in the past, the amount of information aggregated in the databases created after 9/11 is immense. In the past, where the police might have had lists of drivers license numbers and home addresses, the current

generation of information aggregation and correlation systems, such as Seisint's Matrix, store and can connect much more in the way of social networking information (O'Harrow, p.121), thereby putting additional individuals at risk for police abuse.

In the case of Collier County, Florida, it was a lucky break that allowed a problem like that to be "dealt with." Terri Lucas in the Fingerprinting Department at the Collier County Sheriff's Office was fired for unauthorized access to the DAVID system, the database for driver and vehicle information, when she looked up her ex-boyfriend's current girlfriend. The break in the case came when the current girlfriend notified police. Lucas said she looked up "a ton of people…for fun…We used it like a yearbook." The department plans to start running audits against "unusual activity" so that these types of problems can be dealt with (Spinetto, 2008).

An interesting aside in the matter of the London bombing case was the attempt to convict three men for helping to scout locations and training with the bombers, as well as being connected to the apartments in which the home-made explosives were mixed. The government used cell phone tracking data and surveillance footage for travel around London on December 16 and 17, 2004, to show that the accomplices went to the London Eye and Natural History Museum. Prosecutors said the itinerary "bore a striking similarity" to the bombers' travels on the day they blew up the train cars and the bus (Stobart & Rotella, 2008, par. 9). The buried lead is that the cell phone tracking data existed for the suspects. Therefore, everyone's tracking data is saved all the time, and is possibly held indefinitely. It's all up to the cell phone company.

An example of an unsuccessful prosecution because of government lies in the United States was the case of one of the "sleeper cell" prosecutions. This story made the news when Attorney General John Ashcroft announced the arrests of

four Muslim men in Detroit. Unfortunately for the sleeper cell narrative, the charges were dropped quietly when Richard Coventino, prosecutor of the case, was indicted for attempting to enter false evidence into the record, and concealing other evidence (Wolf, 2007, p. 10).

### 3.3. Infiltration

One of the tactics the FBI has been instructed to (re-)adopt is that of infiltration. FBI informants infiltrating, spying on, and in some cases agitating and inciting otherwise peaceful, lawful, protest organizations was one of the strategies that was decried in the Church Committee hearings and subsequently outlawed. A fact of relevance in the wake of the Church Committee Hearings and the fate of the Intelligence Oversight Board that was set up in response to the findings of lawlessness in the law enforcement and intelligence community is that in the recent past, the powers of that board have been severely limited by President Bush (Savage, 2008).

President Ford created the Intelligence Oversight Board as a response to the 1975-1976 investigation by Congress into domestic spying, assassination attempts and other intelligence agency abuses. President Ford's executive order creating the board was effective March 1, 1976. Almost 32 years to the day of its creation, President Bush limited its powers with an order issued February 29 (Bush, 2008), in a move which the timing of was termed "purely coincidental" by the White House.

One major change to the board's operation was that in the past, the board was to inform the President and the Attorney General when an intelligence activity was thought to have been "unlawful or contrary to executive order" (Savage, 2008, par 9). Now, the board is not to refer anything to the Justice Department independently, and only to inform the president if other officials are not

“adequately” addressing the problem. Also, the board no longer has oversight of each agency’s general counsel and inspector general, and instead of each inspector general being required to file a report with the board each quarter, each agency director has the discretion to report law-breaking to the board at those directors’ discretion, with no schedule for notification (Savage, 2008).

Weakening the Intelligence Oversight Board was merely the latest in a series of actions throughout Bush’s terms that have limited and weakened restrictions on intelligence agency activities. Another change allows the NSA to gather information about Americans by using other agencies to collect the information. Assassinations, which were once prohibited, are sanctioned (Savage, 2008, par. 11-12; Yoo, 2006, p.49). Wiretap laws and policies have been significantly weakened. Congress had a law on the books requiring that the full House and Senate intelligence committees be briefed about spying activities, but the administration has determined that only the committee leadership needs to be briefed. And executive orders were once thought to be in force until rescinded, yet the Bush administration has secretly authorized members of the intelligence community to ignore certain executive orders, without actually rescinding the orders (Savage, 2008).

One of the operations to which the creation of the Intelligence Oversight Board was a reaction was COINTELPRO. The Counter Intelligence Program was an FBI operation which used agents and informers to infiltrate and discredit civil rights groups, anti-war groups and other groups whose interests were inimical to the established power structure. For example, on April 22, 1970, the FBI was there when 20 million Americans participated in Earth Day. Agents in 40 cities were ordered to spy on Earth Day gatherings and report on individuals and groups which planned and participated in the Earth Day events. The goal of the FBI was to link the individuals and groups in attendance to organizations which

were targeted for “surveillance, infiltration and disruption” (Cole & Dempsey, 2002, p. 7).

That Earth Day, the FBI in Denver was diligent about recording Senator Gaylord Nelson’s utterances, and had written down each of the slogans on the signs that protesters carried. In general, however, the FBI ended up investigating civil rights activists, Vietnam War protesters, women’s liberation advocates and other protest groups. Some of the more innovative FBI tactics included spreading misinformation about groups, inciting illegal activity and generally trying to discredit the groups and in general bring discouragement to the members of those groups (Cole & Dempsey, 2002).

### 3.4. Surveillance and Interdiction on the Internet

In the U.S. strategy for combating terrorism, one of the venues in which the war on terror is to be fought is the Internet. The United States’ policy is clearly stated, in that, “We will seek ultimately to deny the Internet to the terrorists as an effective safehaven (sic) for their propaganda, proselytizing, recruitment, fundraising, training and operational planning” (*National strategy*, 2006, p. 17). An example of success in that arena is illustrated by the fact that someone, the government would not say who, took down various al-Qaeda sites prior to the anniversary of the 9/11 attacks.

Al Qaeda had been using five main online forums to deliver their messages. All five of these were taken off-line on September 10th, 2008. The next day only one was back up and others were scrambling. The anniversary message did not appear until September 19th, and by then it was not as effective for the terrorist group. This was a serious blow to al-Qaeda’s propaganda effort, as they had been trumpeting the appearance of a video in the weeks prior to the seventh anniversary of the World Trade Center attacks.

U.S. intelligence sources would not say if the U.S. government was behind the attacks, although some speculated that it might have been an independent effort by Web “vigilantes.” Erich Marquardt, of the Combating Terrorism Center at the U.S. Military Academy at West Point, said, “The downside of knocking jihadist Web sites offline is that you lose the ability to monitor jihadist activities” (Knickmeyer, 2008). Clearly then, even the most “obvious” anti-terror strategies may have a downside.

In this particular case, monitoring the Web site for information about that which the jihadists are thinking is different than tracking American citizens’ movements as they go about their daily routines, and thus has value and is a wise use of resources. And, unlike the average American who might join a protest organization or social justice group, some terrorists have more in common with common Internet criminals than social activists.

Thus, a dimension to terrorists’ capabilities, and one which makes the lack of security of the states’ Real ID databases a critical problem, is the fact that terrorists use traditional criminal means to raise money to conduct operations. This means that terrorists will use identity theft and credit card fraud as methods of raising money. Throughout the IT industry it is accepted that any database that can be accessed remotely can be compromised through regular hacking as well as by tricking individuals who have access to a system into divulging their credentials or other means of access (Granger, 2001).

One example of cybercrime by terrorists to raise money is the theft of data by a group of three men. Tariq al-Daour, 21, Waseem Mughal, 24, and Younes Tsouli, 23, pleaded guilty in Britain in the summer of 2007 to charges related to inciting terrorism, specifically to using the Internet to incite murder. What they were really guilty of, however, was a series of cybercrimes involving stolen credit cards numbers taken from victims in phishing attacks (Krebs, 2007).

Phishing is the practice of sending emails to random individuals with a link to a site that looks to be a legitimate site, but in fact steals the credentials that the victim might input at a legitimate site, but due to the phishing, input at the bogus site. For instance, someone might get an email with a link to a site purporting to need information to “verify” their account status, or avoid “cancellation” of a service ("Phishing explained," n.d.). Attacks that are not strictly technical in nature, in that they require tricking a person, are called “social engineering” attacks (Granger, 2001).

In the case of the three terrorists who pled guilty in Britain, one of the individuals who fell prey to the “social engineering” attack was Linda Spence of New Jersey. She entered information into a counterfeit eBay site, and subsequently her credit card was used for $2,000 in fraudulent charges to a business in Portugal. The bad guys in this particular case used 72 or more stolen credit card accounts and registered more than 180 World Wide Web domain names at 95 hosting companies in the United States and Europe. These sites were then used to spread jihadist propaganda and terrorism information (Krebs, 2007).

Another issue that has Western security experts concerned involves applications that would normally be considered tools strictly for hackers and criminals, which are available on the Internet. When these tools are modified and crafted to suit the ambitions of terrorists, however, there is an added dimension of danger.

The “electronic jihad” site, Al-jinan.org, was a terrorist site taken off line in the summer of 2007. It illustrates the problems of security on the Internet in an age of terror, as well as the ability of terrorist sites to avoid detection, even in plain sight.

Al-jinan.org has an application for download named “Electronic Jihad.” The purpose of the computer program is to attack Western sites by using what is known as a denial-of-service attack (DoS). DoS attacks are most well-known

currently in the form of distributed denial of service attacks, (DDoS), which are generally attributed to botnets. Botnets have been in the news as botnets consist of regular individuals' and organizations' computers which have become infected with malevolent software or malware, which allows them to be controlled by criminals. Under the criminal control they can launch DDoS attacks (Glenn, 2003, p. 3).

DoS (and DDoS) attacks attempt to take a target Web site off line by overwhelming the bandwidth or server resources with legitimate looking requests, such as for Web pages. When the volume of these requests is too great per unit time, the Web site is unreachable for legitimate users (Glenn, 2003, p. 2).

The software at al-Jinan.org was not particularly effective for the purposes for which it was written. Security experts, were looking at future attempts by terrorists to craft applications for similar purposes with better technique. Jordan Wiens, senior security engineer for the University of Florida put it best, expressing concern as to what might happen if "if they ever get their act together" (Greenemeier, 2007, par. 8).

# CHAPTER 4. THE TECHNOLOGY OF THE REAL ID ACT

## 4.1. What is the Real ID Act? How did it come into existence?

The Real ID Act was passed as part of Public Law 109-13, with the full title of “Making Emergency Supplemental Appropriations for Defense, the Global War on Terror, and Tsunami Relief, for the fiscal year ending September 30, 2005, and for other purposes.” The Act has the short title “Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005” ("Real ID Act," 2005).

The Real ID Act is Division B of the Act. Title I concerns barring terrorists entry to the United States. Title II is “Improved Security for Drivers’ Licenses and Personal Identification Cards” ("Real ID act," 2005). The Act was signed into law by President George W. Bush on May 11, 2005 (Bush, 2005). In the President’s signing statement, there was no mention of the Real ID provisions of the bill, which meant that the White House would enforce all of the provisions of that part of the Act.

The Real ID Act started out as H.R. 418, entitled, “To establish and rapidly implement regulations for State driver’s license and identification document security standards, to prevent terrorists from abusing the asylum laws of the United States, to unify terrorism-related grounds for inadmissibility and removal, and to ensure expeditious construction of the San Diego border fence.” The bill was then appended as Division B to H.R. 1268, which bears the title of the Public Law which was eventually passed ("H.R. 418," 2005).

The original Real ID Act, as H.R. 418, was sponsored by Representative F. James Sensenbrenner and introduced on January 26, 2005. At that time, he was Chairman of the House Committee on the Judiciary ("Congressman Sensenbrenner, “ n.d.).

There are several aspects to the Real ID Act which deserve consideration. The wording of the Act is vague on the manner in which the goal of the Act is to be achieved. The goal of the Act is that licenses are to be made more secure, and the rule-making fell under the purview of DHS. There was contention regarding the rules and whether RFID was to be used. The current rules do not specify RFID as the vehicle for the machine-readable format. However, critics, among them State Representative Jim Guest of Missouri, contend that the bar code format currently specified could be changed by DHS by fiat to RFID with no meaningful input nor oversight .

## 4.2. What is a Real ID?

A Real ID is a driver’s license that conforms to the rules issued by the Department of Homeland Security (DHS) in 6 CFR Part 37, the Federal Register of January 29, 2008, pp. 5271-5340, entitled, “ Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule.” All of the following descriptions of what the Real ID consists and procedures for issuing the ID, including the format and description of the actual document are contained in the Final Rule.

The rules are constructed to dictate to the states that on a series of dates, the Federal government will no longer accept state-issued IDs that don’t conform to the Real ID rules. For instance, states must have applied for a waiver (extension) on conforming to the federally mandated standard by March 31, 2008, which all of the states did. As of December 31, 2009, if a state has not complied with the

terms of the Material Compliance Checklist and applied for another extension by October 11, 2009, the federal government will not accept those states' citizen's IDs for federal purposes. And on May 11, 2011, the federal government will not accept IDs from states determined to not be in compliance with Real ID. Then on December 1, 2014, those born after 1964 must have a Real ID, and December 1, 2017, the final group, everyone, will have been checked and verified. Anyone without a Real ID will not be allowed to board an airplane, go into a nuclear power plant, enter a federal building, or "such other purposes as established by the Secretary of Homeland Security" (*Minimum standards*, 2008, p.5273). One can only guess as to what the Secretary of the Department of Homeland Security might dictate, and dictate is the correct word, as there is neither judicial nor legislative oversight for implementation of this Act, as State Representative Jim Guest notes (Ferguson, 2007, par. 9).

Quite possibly, most people will not be inconvenienced much by not being allowed to visit a nuclear power plant. However, the rules make for the interesting situation of an American citizen possibly being denied the ability to petition the Federal Government for redress of grievances if they don't have their Real ID with them. Considering that 20 percent of all ID instruments are lost each year (Schneier, 2007, par. 7), it would be inconvenient to actually have gotten it then have it stolen the night before the big court case.

The states shoulder the responsibility for ensuring the validity of source documents which verify the identity of the individual and have rules for document retention. Documents are to be scanned and stored in computer storage, which creates another target-rich environment for hackers.

The ID card itself must have, according to current rules, a 2D bar code as the machine readable zone (MRZ). This will contain a copy of the information printed on the driver's license, and shall include the holder's full name and address, date

of birth and gender, the card's number, and the person's signature. A digital photograph is also mandated, although at the current time it can be color or black and white. The 2D bar code format is the PDF417 format in use by many law enforcement agencies today, and without encryption. This allows for easy access to the information by law enforcement and anyone with a bar code reader (airline boarding passes have 2D bar codes).

### 4.3. Is Real ID an Unfunded Mandate?

Some of the tension between the states and the federal government has to do with the "voluntary" nature of the provisions of the Act and whether it is indeed something with which the states are to voluntarily comply, or if compliance can be considered to be mandatory. If it is not voluntary, as some critics contend, due to the draconian penalties for non-conformance by the states, then it becomes an unfunded mandate. The states contend that the expense of administration to comply with the Act is onerous and that the Act amounts to an unfunded mandate. United States Senator Kahikina Akaka (D-Hawaii) said, "The Act places a significant unfunded mandate on states…" (*Understanding the Realities of REAL ID*, 2007). James Harper of the Cato Institute, a libertarian think tank in Washington, D.C., in his testimony before the Senate Judiciary Committee, also described the Real ID Act as an unfunded mandate (*Real ID Act Hearings*, 2007).

During the late 1970s and early 1980s, mandates were a popular topic of study. At that time, state officials were vocal in their dissatisfaction with federal mandates that were not funded with commensurate federal aid or grants to the states (MacManus, 1991).

Intergovernmental tension is fueled by the imposition of imperatives on lower levels of government by levels of government above, without the necessary

funding to achieve the mandated condition (Leckrone, 1997). The imposition of unfunded mandates is not necessarily uniquely federal to state in nature. The intergovernmental tensions were felt in the state to county hierarchy to such a degree that by 1990, with the addition of Florida and Wisconsin, ten states had constitutionally mandated reimbursement provisions and eight states had statutory requirements to reimburse local governments for state mandates (MacManus, 1991). By 1998, totals had grown to 12 states with constitutional and 13 with statutory provisions regarding mandates (Nobles, 2000).

In 1995, the Unfunded Mandate Reform Act (UMRA) was signed into law, which had as its stated purpose, "…to strengthen the partnership between federal, state, local and tribal governments by ensuring that the impact of legislative and regulatory proposals on those governments are given full consideration in Congress and the Executive Branch before they are acted on" (Leckrone, 1997, p. par 4).

In hearings conducted in May of 2007 by the Senate Committee on the Judiciary, Senator Patrick Leahy (D-Vermont) and Senator Arlen Specter (R-Pennsylvania) both quoted the DHS estimate of costs to the states for compliance as $23 billion (*Real ID Act Hearings*, 2007, pp. 2-3). In September of 2007, that estimate was revised down to $11 billion over five years (Lipowicz, 2007).

At a press conference announcing the final rules for Real ID, Michael Chertoff continued to put pressure on states to comply. Secretary Chertoff threatened that if individuals are carrying ID from states which did not comply nor intend to comply with the Real ID Act, those individuals would not be allowed to fly on commercial airlines, nor to access federal buildings (Chertoff, 2008b).

A selling point for Real ID as the Secretary tells the story is that the adoption of Real ID will help ameliorate the illegal immigration problem. His contention is that

illegal aliens use Social Security Numbers of citizens, thus presenting a fraud and identity theft problem (Chertoff, 2006b, p. par. 12) and that the use of Real ID will solve that problem. Secretary Chertoff also made the case for expanding the scope of use for Real ID for employment purposes, by integrating the information that employers checked against Basic Pilot/E-Verify with the Real ID distributed database. Basic Pilot, now rebranded as E-Verify, is a program of cooperation between the Social Security Administration and the Immigration and Custom Enforcement department of DHS which allows employers to check Social Security Numbers to see if they match the names that applicants provide (DHS Basic Pilot /E-Verify Program, 2008). Secretary Chertoff asserts that Basic Pilot does not indicate if that Social Security Number is possibly being used in multiple employment situations, but that if the database used for identification were used in conjunction with the Real ID database, having been referred for action through DHS, this would protect people from identity theft (Chertoff, 2006b, pp. par.16-19).

Other mandates to the states for compliance with the Real ID Act include deadlines for compliance, and privacy and data security considerations. States' rights adherents and civil libertarians observe that national identity cards are anathema to the citizens' sense of the role of the federal government. Even as DHS has pushed the deadlines back, the Secretary of the Department of Homeland Security foretells of severe punishment for the residents of the states that do not comply with the Act. The same punishment was to be meted out to states that missed even the deadlines for requesting extensions for compliance dates.

In the final rules as DHS released them, states had until May 11, 2008 to either comply with the Real ID Act or request a waiver for extension of the deadline. After that date, individuals from states that were not in compliance nor had applied for a waiver of compliance would be subject to "secondary" treatment at

airports and upon entering federal facilities. This would entail pat-down searches (Singel, 2008a) and the need for DHS to perform some type of verification to assure the identity of those individuals. This type of situation would also cause delays, which Secretary Chertoff hypothesized would translate into dissatisfaction of the citizens with their non-compliant state governments, and thus promote compliance (Chertoff, 2008b, pp. par. 57-58).

Privacy advocates claim that the Real ID Act's inclusion in the Tsunami Relief and Defense Appropriations Bill was done stealthily and the time frame was such that it was only a matter of days before the vote that those civil libertarians who would oppose the Act even knew it was included, limiting their ability to respond and attempt to remove the Real ID portion from the larger bill. Twelve Senators went so far as to write a letter to then-Senate Majority Leader Bill Frist urging that the Real ID portion of the Act not be included in the larger appropriation bill, but to no avail ("Twelve Senators urge Frist" 2005).

In addition to the features of the Real ID cards described earlier, there is another component to compliance with the Act. Concurrent with the issuance of the cards with the 2D bar codes, the individual's identity information would be stored in a database in each state. This data would be stored in a format such that the databases for each state could communicate for lookup purposes with each other state, and such that all states would have database formats that would be interoperable between all other states ("Real ID draft," 2007). The states would be required to store electronic images of the source documents for 10 years or paper copies of the source documents for seven years ("Real ID Act," 2005, p. 49).

## 4.4. Timing and Implementation Complications

Real ID Advocates, including Michael Chertoff and in the testimony to the Senate Judiciary Committee, Janice Kephart of 9/11 Security Solutions, LLC, suggest that the driver's license provisions in the Real ID Act is superior to the driver's license provisions in the 2004 Intelligence Reform Act. The Senators at the hearing, on being concerned about the fact that the Real ID Act was pushed through in an authorization bill without hearings, asked what made Real ID superior in the security requirements for driver's licenses to those in Public Law 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, which had gone through the hearing process and was considered to be in line with the 9/11 Commission recommendations ("Intelligence reform," 2004).

A close reading of Section 7212 of Public Law 108-458 of 2004 reveals that the most significant difference regards the mandate for a national distributed, searchable database. The Intelligence Reform Act does not require such a database, whereas the Real ID Act requires that database to be implemented ("Real ID act," 2005, p. 50). The database requirement is known in the Act as the "Driver License Agreement" (DLA). Another difference is the Real ID Act's requirement to cross-check the individual's identity against the database of Social Security numbers ("Real ID act," 2005, p. 49). The DLA does not extend only to the states and federal government, but also to "…those provinces and territories in Canada and those states in Mexico that join the DLA and comply with its provisions. While it's not specifically stated, other countries could join the DLA, which would mandate reciprocity of information on potentially a global scale." (Ferguson, 2007)

Another significant difference between the driver's license provisions in the Real ID Act and those in the Intelligence Reform and Terrorism Prevention Act of 2004 exists. This is that the rule-making falls solely under the purview of the Department of Homeland Security. This scuttles the provisions of the 2004 Act

which had the states and the federal government working together to arrive at standards for driver's license security.

There was confusion when the law was passed as to what mechanism would be used for the machine readable format of the Real ID card. Many in the industry at the time thought that RFID would be the front-running technology (Ferguson, 2007), as passports were being redesigned and issued with RFID chips starting on August 14, 2006 (Ezovski & Watkins, 2007, p. 16).

The entire story of the Real ID Act is unusual for many reasons. One would expect that there would be consensus in the passage of a law which would help keep the American public safer. It appears, however the Real ID Act is something that is being forced on the people of the United States, as demonstrated in the threatening stance taken by representatives of DHS.

Secretary Chertoff did nothing to dispel the notion that DHS was using heavy-handed tactics in dictating to the states the manner and timing with which the Real ID Act was to be implemented. In an editorial published soon after the final rules were released, dismissing criticism of the manner in which the rules were to be implemented, he wrote, "A good example is the spurious claim that we're ushering in a national identity card. What we are actually doing is setting standards *that will let the states keep issuing their own ID cards*." (emphasis added) (Chertoff, 2008a) The implication is that even though this is not a national ID card, that if the states do not follow the mandate, they would not be able to continue to issue their own ID cards.

Throughout the process of attempting to get the Real ID initiative off the ground, there has been confusion regarding the deadlines and with what parts of the law states were to comply at what time.

On September 10, 2007, Secretary Chertoff told the Senate Committee on Homeland Security and Governmental Affairs that the states were originally given a deadline of October 1, 2007, to comply even though the final rules had not been issued yet at that time. The date was moved back for states requesting a waiver to the end of 2009 (Lipowicz, 2007). But adding to the confusion was the fact that in the meantime, May of 2008 was set as a deadline for having all states either come into compliance with Real ID, or apply for a waiver. In November 2007, Secretary Chertoff revealed a new timetable, which would have changed the states' target of 2013 for having 245 million U.S. driver's licenses comply with Real ID in such a way as to make the target date 2018 for drivers older than 40 or 50 (the drivers' age break point hadn't been determined at the time) to get Real ID compliant licenses (Hsu, 2007b).

At that time, Timothy Sparapani, senior legislative counsel for the American Civil Liberties Union, noted that DHS was continually weakening the program to attempt to gain compliance. Sparapani said, "DHS is doing back flips in order to get states to say they are complying with Real ID" (Hsu, 2007b).

Secretary Chertoff and DHS had set a compliance date for the states of May, 2008, even before the Notice of Proposed Rulemaking (NPRM) had been issued. The NPRM appeared in the Federal Register on March 9, 2007 ("Real ID draft," 2007). Yet in February of 2007, Michael Chertoff testified to the Senate Homeland Security and Governmental Affairs Committee and said he was "pretty adamant" about a May 2008 deadline. Senator Susan Collins (R-Maine) was considering sponsoring an amendment giving the states more time. She observed, "It has been two years since the Real ID Act passed, and yet we don't have detailed regulations or guidance from the department setting forth the standards that the states are going to have to follow" (Hudson, 2007, par. 5).

Secretary Chertoff made the point that privacy and security were paramount and said, “I do want to make it clear that one of the reasons it’s taking awhile is we have actually done quite a bit of consultation even in the preliminary stage with state officials and privacy advocates and other folks” (Hudson, 2007). Secretary Chertoff never enumerates who the privacy advocates and “other folks” might be. A reasonable person might presume that because the program is a security program and security of the data and the computers holding the data is important, the “other folks” might be computer and information security professionals.

## 4.5. The Race/Ethnicity Field

Secretary Chertoff left the door open for the inclusion of biometric identifiers – beyond the digital photo requirement. Each driver’s license will have at a minimum a digital photograph as the biometric identifier. As the Secretary indicated at the press conference upon release of the final rules for compliance with the Act, DHS was not opposed to other biometric identifiers being included on the ID (or in the database), “We have nothing against a fingerprint. Some states have fingerprints, some states don’t” (Chertoff, 2008b).

The Act does not specify that a race field be included, nor filled. In addition to the digital photograph, the Act mandates the individual’s full legal name, date of birth, gender, driver’s license number, address and signature ("Real ID act," 2005, pp. Division B, Title II, Sec. 202, (b)). The Act mandates that the machine-readable portion contain common data elements. This is of special concern for civil libertarians as there is a race field in the specification for the machine-readable portion of the Real ID that DHS has picked for implementation. At the time Jim Harper spoke to the Senate Committee on Homeland Security and Governmental Affairs, subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia on March 26, 2007, the Notice of

Proposed Rule Making (NPRM) that DHS promulgated for the implementation of Real ID specified the machine readable portion to consist of a 2D barcode, the PDF417 standard. The NPRM, being the period in which interested parties and the public could comment, was an opportunity for Jim Harper of the Cato Institute to highlight the fact that there is a race field in the format specified by DHS. The specified format DHS proposed in the NPRM is the 2005 AAMVA Driver's License/Identification Card Design Specification, Annex D (Harper, 2007).

Critics of the Act suggest that there is rarely a field which is specified which will be left blank. Harper notes that DHS does not require all of the fields to be developed in the standard, and certainly doesn't specify that the race field be developed – but also that "DHS has done nothing to prevent or even discourage the placement of race and ethnicity in the machine-readable zones of this national ID card." (Harper, 2007, p. 212) Mr. Harper was adamant in his objection to the inclusion of a race field, urging DHS to mandate that the field not be used, stating on the record:

> Avoiding race- and ethnicity- based identification systems is an essential bulwark of protection for civil liberties, given our always-uncertain future. In Nazi Germany, in apartheid South Africa and in the recent genocide in Rwanda, horrible deeds were administered using identification cards that included information about religion, about tribe, and about race. Implementation of the REAL ID Act, which would permit race to be a part of the national identification scheme, would be a grave error. (Harper, 2007, p. 212)

In the final rules, DHS responded to concerns about the race field being included and possibly used – but did not specifically indicate that the race field was not to be used. In the response to a comment regarding the use of a race field in the final specification, DHS wrote:

> Race is not a data element contemplated in this rulemaking and the reference in the NPRM to the AAMVA standard was not intended to include race as a data element in the MRZ for REAL ID. (*Minimum Standards*, 2008, p. 5305)

However, the next paragraph states:

> The final rule sets the minimum standards to include, but recognizes the authority of the individual States to add other elements such as biometrics, which some currently include in their cards. (p. 5305)

This is not a repudiation of the inclusion of a race field. In the response to the next comment, DHS again attempts to downplay the data element of race, without specifically prohibiting the states from using that field, stating:

> DHS disagrees with the notion that the standard selected should be rejected because it includes coding for race. DHS has never stated that race should be encoded on the license, and specifically stated in the proposed rule that it was not incorporating wholesale the card data elements currently required by the AAMVA. (p. 5305)

According to the specification, at D.12.3.2, the Race field (k), Data Element DCL, the race field is already an optional element. All of the fields in D.12.3.2 are optional, as the "required" fields are listed in Section D.12.3.1, "Minimum mandatory data elements." ("Personal identification," 2005), so the last sentence in the final rules is questionable either in its accuracy or pertinence. If DHS, which mandates every part of the Real ID implementation, down to the exact date of each step of compliance, were to state that the race field would not be used, it would not be used. The rules specify what documents to accept, how and how long they are to be stored, what the machine readable zone will incorporate, what databases individuals' identities will be verified against and what type of photograph to use. If the Department of Homeland Security mandated that the race field was to not be used, it would not be used.

Alternatively:

> …white people would carry the designation "W"; black people would carry the designation "BK"; people of Hispanic origin would be designated "H"; Asian or Pacific Islanders would be "AP"; and Alaskan or American Indians would be "AI." (*Will Real IDs*, 2007, p.175)

By not prohibiting its use, it is left to the individual states to use that field and it will be part of the MRZ for all citizens of whatever states elect to use it, if not tomorrow then the next day.

## 4.6. The 2D Barcode and its Security

For instance, Randy Vanderhoof, Executive Director of the Smart Card Alliance, an industry trade group which, among other activities, organizes the trade shows, such as the annual Smart Cards in Government Conference, wrote to express disappointment in DHS's choice of a 2D bar code, i.e. the PDF417 specification during the NPRM phase of the rulemaking process. He wrote, of the proposed specification:

> This is where the document and DHS recommendation fall short. The core reason for the REAL ID legislation in the first place was supposed to improve security, not the least expensive solution for storage and transmission of data that states could agree on. (Vanderhoof, 2007, par. 2)

A glance at the Standards for U.S. License Technology table underscores the point – as 44 states and the District of Columbia are using 2D bar code technology. The states that are not are California, Michigan, New Mexico, Ohio, Texas and Wyoming ("Standards," 2008). An interesting aside is that Wyoming is the home state of Vice-President Dick Cheney, and that is the only state that uses no magnetic stripe, 1D or 2D bar code technology.

As a leading light in the industry, the Executive Director of the SmartCard Alliance also writes that DHS in the NPRM phase of rulemaking did not address the issues of tampering, counterfeiting or duplication of documents for a fraudulent purpose, even though the opening summary of the proposed rules stated that these issues would be addressed (Vanderhoof, 2007). In the final rule, in Section 37.15, DHS pushes the responsibility for these action items off onto the states, with the caveat that the states must provide DHS with written reports specifying the manner in which these goals will be. At the same time, the regulation specifies that the information will be considered SSI, or Sensitive Security Information, which "must be handled and protected in accordance with 49 CFR part 1520" (*Minimum standards*, 2008, pp. 5334-5335).

Therefore security and anti-tampering information falls under the purview of the Transportation Security Administration, as Title 49 is Transportation in the Code of Federal Regulations, and two important effects are immediately felt. Only persons with a “need to know” will receive the information (1520.11) and there is no release of the information under the Freedom of Information Act (1520.15 (g)) ("49 C.F.R. Part 1520," 2004) This puts the information as to how the Real ID’s are to be safeguarded against tampering outside the possibility of any type of independent review by members of the public, industry or academia. It also means that those who know what the safeguards are supposed to be, even if they find those safeguards deficient, cannot take the information to the public, and force a security solution through publicity.

It is sometimes argued that “security through obscurity” is useful. Security expert Eugene Spafford, Ph.D., director of the Center for Education and Research in Information Assurance and Security and an Association of Computing Machinery (ACM) Fellow (Cooper, 2001), has written on the subject and has come to the conclusion that prevails in the computer security field, which is that it does not work (Spafford, 2008). It may work for awhile, and depending on the importance and determination of the adversary, it may work indefinitely. (Think of the case of some obscure custom computer program written for a small office which runs on a computer not connected to a network and compare that to security for a database (or distributed database) holding millions of credit cards, or better yet, names, dates of birth and permanent addresses.) However, if the target is of value, attackers will attempt to compromise the security of the system.

The motivation of the entity compromising the security of whatever system is being attacked must then be examined. This motivation will dictate how widely the knowledge of the vulnerability and exploit will be disseminated. The continued security of the system depends on how widely the knowledge of the vulnerability and exploit is disseminated. Some attackers may want to keep the

exploit to themselves, assuring repeated success. In the case of Real IDs, success would be measured by forging Real IDs and/or modifying the database(s). Some attackers may publish their discoveries of security vulnerabilities, allowing for wholesale destruction of the security of the system. In the meantime, secrecy regarding the insecurities of the system will adversely affect the public, which is every American citizen and those citizens of the North American Union who live in states that are part of the trans-national Driver's License Agreement (DLA).

There exists at least one inconsistency between the Real ID specification which DHS published in its final rules and the format as the PDF417 standard is written, as well as inconsistency within the format. One inconsistency has to do with the use of the null data elements for unknown or unavailable data. In the FAQs on the AAMVA site for the format, the question has to do with the reading of paragraph D.12.3, which states that for optional data elements were the information is not available, "NONE" should be inserted into the field and for mandatory data elements, "unavail" should be recorded in that data field. The question concerned the situation in which the field is shorter than the null identification element, possibly causing the shortened 'N," "NO," or "NON," or "u," "un," "una," "unav," "unava," or "unavai" to be mistaken for some other code ("AAMVA card," 2008, pp. 'Bar Code Format, 2.'). The FAQ answer indicates that the matter is under study. This diverges from the DHS rule which states in Section 37.17 (a) that if an individual has only one name, the single name should be placed in the "last name or family name" field, leaving the first and middle name fields blank. The rules specifically prohibit the use of "place holders" such as "NFN, NMN and NA." (*Minimum standards*, 2008, p. 5335) In this case the DHS place holders do not match the AAMVA PDF417 standard.

Bruce Schneier, a security expert, well-renowned in the information security field and an expert who comments on all matter of security issues, testified in the May

2007 hearing before the Senate Judiciary Committee and made some observations on the general security of the Real ID, and how trustworthy those cards would be. In his statement to the committee he pointed out several problems with the supposed security of Real ID. He noted that the ID could be no more secure than the documents used to procure the trusted ID. This meant that if a terrorist or criminal could not bribe a DMV clerk, the bad guy would try to forge source documentation or bribe a clerk at some agency which would produce the source documents for the ID (*Real ID act*, 2007, pp. 234-235).

Schneier testified to the committee that other problems could result from the existence of shadow databases. These databases would be written to by commercial entities every time the Real ID would be used in a commercial context, just as driver's licenses are now. Schneier brought up the case of lost Real IDs. With the knowledge that 20% of all identity documents are lost per year, he warned that any parallel or separate system for re-issuing lost IDs would also be susceptible to abuse. Another issue is that of a terrorist or criminal impersonating a law-abiding citizen. In this case, the question of the identity documents is similar, and in that instance the terrorist or criminal would be able access more easily the restricted spaces that the use of Real ID was supposed to protect. The poignant observation from Bruce Schneier: "And if you think it's bad for a criminal to impersonate you to your bank, just wait until a terrorist impersonates you to TSA." (*Real ID act*, 2007, p. 237).

The more trusted a form of identification, the greater access the identification gives. Those who would forge an ID will be able to access more and better information and physical spaces when they forge a more trusted ID. In the United Kingdom, a country in which national identification cards have been issued and databases centralized, there is debate over the wisdom and efficacy of issuing national ID cards. A report from the London School of Economics takes issue with the British government's assertions and assumptions regarding the national

ID. The report indicated that as ID's become more secure, those who would break the security and forge cards are becoming more resourceful:

> Even as the cards are promised to more secure, attacks become much more sophisticated. Most recently, Russian security agents arrested policemen and civilians suspected of forging Kremlin security passes that guaranteed entrance to President Vladimir Putin's offices. (Rotenberg, 2006, p.128)

The purpose of Real ID is to be the most trusted ID and DHS envisions that it will be used for employment verification, and for all of the uses driver's licenses are used for now. With the convenience of bar code, for now, and possibly RFID in the future, it will be used for all manner of transaction. Even as the government attempts to anticipate forgery and forgers, as Bruce Schneier explained in testimony before the Senate Judiciary Committee, the new twenty dollar bill was forged before it even hit the streets (*Will Real ID*, 2007, p. 234). With this being the case, and with the large numbers of ID cards which would have to be replaced when enemies forge Real IDs, there has to be acceptance of the fact that the criminals and terrorists with the most resources will be most able to breach the security of the Real IDs. And if this is the case, then the purpose of the Real ID cannot be for preventing terrorism, except of the lowest level, most casual kind. The people who will be using valid Real IDs will be law abiding citizens, and they will be the individuals that the nationwide surveillance system will track.

## 4.7. Computers, Databases and Security

One of the most intrusive and disturbing aspects of the implementation of the Real ID Act is the requirement that all states' databases be searchable by every other state and the federal government. This creates a situation which is more insecure than creating a large centralized database in terms of safeguarding the data, but with the level of intrusiveness of a national ID database in that the data is all in one place (logically or virtually, as opposed to physically) through the

ability to search distributed databases from multiple locations and entities. In computer parlance, to say it is logically in one place means to the computer's logic, it doesn't matter if it is physically all in one computer system located on one sub-basement. The computer's logic, with the connections that the computers make with each other, and the speed of access and the speed with which the data can be moved from one computer to another, to the computer, the database is one "logical" entity. Just as the university computer and the Yahoo computer and your computer at home are not in the same place, if you didn't know that, you might think that they were.

Almost everyone in contemporary society has an idea of what a computer is and what it can do. Computers are good at doing the same thing over and over, as opposed to doing something unique each time it is called upon to do something.

A database system can be thought of as a computerized record-keeping system. The foundational building block in the construction of a database is a "record." A record is a set of data, of which an example would be the set of data stored in the 2-D barcode mandated in the rules for Real ID. When it becomes necessary to organize these records, they are stored in a database (Date, 1995).

Records have structures defined by the database designer(s), and each of these groups of records with the same structure is stored in a "table." A database can have many tables, and data fields in some tables may provide the links to other tables. These other tables may have records with different structures and may be filtered and sorted in different ways than the original table, but have information taken from the other tables (Date, 1995). In the example of Real ID, and the state DMV databases that make up the foundation for the distributed database, each record would be keyed to an individual. The key field in a record is a unique identifier and is the field on which the records are sorted. There are occasions when a key is composed of primary and secondary fields, but for all intents and

purposes, the operation of the database should be transparent to the end user. In other words, when the policeman or the coat check girl scans your Real ID, they don't need to know how the database is designed, or that the local database they are creating of their encounter with you is first checking a statewide database for your information, then the database in your home state (assuming those are different) and then their marketing databases and then whatever watch list databases the FBI or CIA or other member agency of the intelligence community dictate must be checked. They just know that when they scan the machine readable zone that your picture and date of birth and home address and quite possibly race come up, so that they know it is you (according to the computer) who they are stopping randomly or to whom they are giving your coat. For purposes of each state's database, it is hoped that each individual will have a unique driver's license or ID number (or alphanumeric identifier). But the policeman and the coat check girl don't need to know how the databases are designed or link, nor do they want to know. So then, after your time and location have been logged into these multiple databases so NSA can run an algorithm against your movements to see if you are doing terrorist things, you might be able to go on your way. Then again, if you are traveling over the same ground a criminal or terrorist traveled, in the same order, you might have some explaining to do – to the computer at the police station.

As each new individual is assigned a driver's license number, the data is entered and a number of record-keeping functions occur. The mechanics vary between implementations, and this is where the real world meets the world of computer science. The idea of the Real ID act is to produce a system in which each individual would have only one driver's license or ID card, regardless of state, at a time. Various mechanisms are to be employed, including checking against a database of Social Security numbers, various immigration databases, a system which is not up yet with vital events (such as births and deaths), etc. The trick for normalizing the data has to do with names, numbers associated with birth

certificates in various jurisdictions, and the data in these other databases. Informally, normalizing the data refers to the process of combining or discarding, depending on the desired result, information from duplicates entries in databases in well-defined ways (Date, 1995).

Once the data is in the database, stored in fields that are organized into records in tables, users are going to want to query the database. Generally, Structured Query Language (SQL) with possibly some variation is used. Also, users with the correct privileges and access rights to a database can change or input data. When one table has a field in a record which is changed, it is useful to have other tables with the same fields, whatever the record and table format, change also so that the data is consistent.

A relational database management system (RDBM) updates all of the associated tables when a field that appears in more than one table changes. The term relational refers to the fact that data fields in certain tables relate to, or are informally correlated with, the same data fields in other tables, just in a different record construct.

Modern (RDBMSs) have graphical front-ends, so that users can construct queries without too much trouble. For the average user of the Real ID database system, however, the swipe of the 2D barcode will automatically query the database. The mechanism should be such that the state the Real ID is registered with will be first to be queried.

For more advanced users, who want to correlate data from the card swipe with other data either from that database or in others, the query capabilities would be much enhanced. In the commercial world, data aggregators such as Axciom, ChoicePoint and LexisNexis use extensively correlated databases such that they

can query across several sources of information and find intersections, quickly and easily (Behar, 2004).

Then there is Seisint. Even pre-9/11, correlative power of commercial databases was well-developed. O'Harrow (2005) tells the story of Hank Asher discovering the power of the database technology he helped build. Two days after 9/11, Asher was at his house with Bill Shrewsbury, a special agent with the Florida Department of Law Enforcement socially, when it struck him to see if he could profile the terrorists using the tools he had at his disposal. He narrowed the list of suspicious characters, according to the data, to 419 before he called a friend of his, Tim Moore, commissioner of the Florida Department of Law Enforcement (O'Harrow, 2005, pp. 98-100). Ultimately, he produced a list 1,200 people who looked interesting. Five of those were evildoers who crashed airplanes into the World Trade Center. This number was achieved after knowing the attack had occurred, and this analysis produced a 99+% false positive rate (Jonas & Harper, 2006). So in this case, it was not predictive data mining, but data mining in hindsight. Naturally law enforcement was very interested and for weeks afterward, law enforcement accessed those databases at no charge, and most probably are paying premium prices to access that information today.

At the end of the process, DHS envisions a system in which each person in the real world is associated with only one identifier in the computer's database, so that all the vital information about that person can be linked to in other databases, or, depending on the semantics, linked to in the relational database management system (RDBMS). The idea of constructing a network of databases, a distributed database, in which the information could be accessed quickly, is the foundation for Acxiom's business model. One of John Poindexter's aides at the Total Information Awareness Office wrote that, "Ultimately, the U.S. may need huge databases of commercial transactions that cover the world or certain areas outside the U.S. Acxiom could build this mega-scale database" (O'Harrow, 2005,

p.61). Acxiom officially suggested a different approach so as not to alarm the public, which was to “use networks to link those data systems together” (O’Harrow, 2005, p.61).

In terms of the massive distributed database that the Real ID Act would create, Bruce Schneier in his testimony to the Senate Judiciary Committee was being generous when he testified that, “Computer scientists don’t know how to keep a database of this magnitude secure” (*Real ID Act Hearings*, 2007, pp. 235-236). The fact is that computer scientists are struggling to come up with a theoretical model for keeping a computer secure, let alone a network or database of any size. There are issues that range from the inherent insecurity of the underlying operating systems and the network protocols they use to communicate over a network, to the fallible humans that maintain and access the data the computers store.

Unauthorized access can mean many things. At the minimum it can mean individuals who have access to the system and data for specific purposes, looking at data at which they are not supposed to look. An example of this type of unauthorized access would be an IRS employee, with legitimate access to the system storing tax returns, looking up the tax returns of celebrities when there was no legitimate job-related reason to do so, as John Snyder was convicted of doing (Coombes, 2008).

It can also mean some actor or organization gaining access when the system security was set up to stop those actors or organizations from accessing the system or data. Examples of this type of unauthorized access can be found in the description of any database breach, an example of which would be the TJX data breach in which at least 45.7 million credit and debit card numbers were stolen (Abelson, 2007).

Data breaches in commercial, educational and government databases, and other losses of data, are in the news constantly. It is patently absurd to think that somehow the data in the database that the Real ID Act mandates would somehow be more secure. If anything, the data will be much less secure, due to the pressures on the administrators to keep their data available.

As the director of the Center for Education and Research in Information Assurance and Security (CERIAS) said in 1989, “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts” (Spafford, 2006). Not much has changed since then to give the industry hope that things are more secure. Events have indicated that systems have more valuable information to steal and are breached on a regular basis.

Almost any week, the news provides an example of the enormity of the problem of keeping information secure. There is a database of database breaches kept by the Privacy Rights Clearinghouse. By its count, from January 2005 to January 2009, the number of compromised records containing personally identifiable information is 251,154,069 ("A chronology," 2009).

## 4.8. States’ Resistance

Several states have resisted the imposition of the Real ID Act and its provisions on their procedures and processes for issuing driver’s licenses. This resistance has taken various forms. For example Missouri State Representative Jim Guest sponsored a bill which would have made Missouri actively non-compliant with the Real ID Act in Missouri’s 94th General Assembly ("House bill no. 1716," 2008). The bill specified, among other provisions directly challenging the Real ID Act’s specifications:

> The department of revenue shall not amend procedures for applying for a driver's license or identification card in order to comply with the goals or standards of the federal Real ID Act of 2005, any rules or regulations promulgated under the authority granted in such act, or any requirements adopted by the American Association of Motor Vehicle Administrators for furtherance of the Act. (Section 3)

The bill never made the calendar for passage in that Missouri congressional session ("HB 1716," 2008).

Representative Guest and others felt that the Real ID Act was an infringement on privacy, so they appealed to the original values of the Founders. Representative Guest said, "We're supposed to be a government of, by and for the people. Government's role is to protect citizens' freedom. In this case they're not doing that. [The Real ID Act] is a direct frontal assault on the freedom of citizens when [the U.S. government] wants us to carry a national ID" (Ferguson, 2007b, p. 16).

Another example of resistance involves the state of Montana. In January of 2008, Montana Governor Brian Schweitzer (D) wrote a letter to DHS saying that Montana was not complying with the Act and had no intention of doing so. He urged the governors of 17 states that had given indications of resisting the federal government's Real ID mandate to join with Montana and force a showdown regarding the May 11 deadline DHS set for compliance or for states to apply for a waiver (Schweitzer, 2008). Georgia was one of the states which had been strongly opposed to the Real ID rules.

DHS spokesperson Laura Keehner was nonplussed when the possibility that all the Georgians traveling through Atlanta-Hartsfield airport, the world's busiest airport, would have to go through secondary screening. "That will mean real consequences for their citizens starting in May if their leadership chooses not to comply. That includes getting on an airplane, so they will need to get passports" (Singel, 2008a).

The issue of states resisting DHS's Real ID-mandated requirements stems also partly from the fact that there had been cooperation between the state and federal government in attempting to set rules for driver's license issuance prior to passage of the Real ID Act. Governor Schweitzer specifically took umbrage to the fact that with the passage of the Real ID Act, the rule-making was unilaterally and precipitously given over to DHS. The Governor urged in his letter that states rally around the passage of S. 717 and H.R. 1117, acts which would reinstate "a negotiated rulemaking process that was on track to improve ID security" (Schweitzer, 2008). He sent that letter to the governors of Colorado, Georgia, Idaho, Maine, New Hampshire, Oklahoma, South Carolina, Arizona, Hawaii, Illinois, Missouri, Nebraska, North Dakota, Pennsylvania, Tennessee and Washington (Singel, 2008a).

In March of 2008, it was revealed that DHS granted a waiver to Montana, in essence stating that Montana's governor's letter was tantamount to a request for a waiver (an extension in the time to comply with the Act.) Governor Schweitzer said in reply, "I sent them a horse and if they want to call it a zebra, that's up to them. They can call it whatever they want, and it wasn't a love letter" (Singel, 2008b, par. 5). Additionally, on the issue of how the government was going to keep the information secure in this distributed database, the governor said, "They tell us it's safe. Tell that to the passport people" (Singel, 2008b, par 8). The reference to the "passport people" involved unauthorized access to passport information perpetrated by contractors at the State Department. These contractors were accessing the passport information databases for information regarding past travel of political candidates (Jones, 2008). Presumably there were fewer people authorized to view the passport database information than would be authorized to access the Real ID database collection, so the conclusion that Governor Schweitzer was drawing was that if an entity comparatively small such as the State Department could not guarantee the safety of the data in the

passport control database, how could anyone assume that the data held in the Real ID database would be safe from unauthorized access?

Replying to the governor through the press, Assistant Homeland Security Secretary Stewart Baker said, “We’re not in the business of asking states to say Uncle. We’re in the business of trying to improve driver’s license security” ("States Challenge Homeland Security's ID Deadline," 2008).

This type of flip rhetoric is also the type of rhetoric that the states, and specifically Governor Schweitzer, objects to. The Governor wrote:

> Secretary Chertoff’s remarks yesterday [January 17, 2008], albeit about WHTI, not Real ID, reflect DHS continued disrespect for the serious and legitimate concerns of our citizens. I take great offense at this notion we should all simply “grow up.” (Schweitzer, 2008)

Other examples of that type of rhetoric in Secretary Chertoff’s utterances included the statement at the final rules press conference in response to a question about putting so much trust in a single piece of identification, “…under that theory we should eliminate passports and let people come across the border using a note written by their third-grade teacher” (Chertoff, 2008b, par. 84).

During the same press conference Secretary Chertoff basically described the driver’s license itself as useless for identification purposes. According to Secretary Chertoff, if a state did not adhere to the new Real ID specification it would “…send a message to people that basically says a driver’s license is useless, it has no identification value, and it’s the kind of thing you can pick up at, like, an amusement park when you pay a few bucks and they do some kind of funny identification” (Chertoff, 2008b, par. 75) This type of statement would serve to rankle Governor Schweitzer, in that the Governor makes the point that Montana driver’s licenses are already more secure than the Real ID Act standards call for, and in a more timely manner. As the Governor said, “We

already have an ID system they are hoping to get to in seven years" (Singel, 2008b).

Elected officials in other states have expressed misgivings about Real ID. The Idaho Senate in March 2007 passed Joint Memorial 3, after the House had unanimously passed it, which was a resolution to refuse to comply with the Real ID Act. Governor Mark Sanford of South Carolina urged his legislators to resist compliance, noting that it would cast the state $25 million to comply initially, and an extra $11 million per year thereafter (Zalud, 2007).

Some states are headed in the direction of compliance with the Real ID Act. According to Secretary Chertoff, at the time the final rules were released, 40 percent of individuals lived in states which were starting to come into compliance with the Real ID Act (Chertoff, 2008b). Some states were moving further, issuing an identity instrument commonly known as the enhanced driver's license. Vermont is one such state and will start issuing these IDs starting in early 2009 ("Vermont issues," 2009).

This Enhanced Driver's License would ease the cross-border movement of individuals under the terms of the Western Hemisphere Travel Initiative (WHTI). Starting in 2008, United States citizens who traveled to Canada or Mexico needed passports or some type of WHTI compliant document to have crossed the border back into the United States. For travel to and from Canada, Mexico and other countries that are part of the WHTI, Vermont and the states of Washington and Arizona are working with DHS to enhance the security of their driver's licenses ("Proposed 'enhanced' licences," 2007). These Enhanced Driver's License and identification cards (EDL/IDs) would contain RFID chips, similar to the chips contained in U.S. passports. Holders of these enhanced driver's licenses can produce them when needing to produce a WHTI-compliant

document, or government-issued photo ID and proof of citizenship to cross the border (K.C. Jones, 2007b).

### 4.9. Increased Scope of Use

Secretary Chertoff and other spokespersons for DHS have had it both ways in the rhetoric. There is an insistence by the department that it is for federal purposes, that it is a way to make people safer on airplanes, in nuclear power plants, and in federal buildings. The idea being that if the person who the ID says is holding it has made it to the door of the conveyance or building, then it is ok for them to pass through that doorway. But it is not enough for a person to have the ID to pass through the doorway. Security personnel frisk the person anyway; to inventory and inspect the contents of the citizen/subject's purse, wallet, computer bag, and pants pockets. Security will conduct this search, if not by physically turning those items or pockets inside out, then with machines that look through the fabric, record the images and display those images for the guards to conduct a visual inspection. Simultaneously, there is insistence from the Department of Homeland Security that there will be other uses for the ID, probably employment verification for a start. So the question again becomes, how is the Real ID Act a measure to stop terrorism more than it is a measure to facilitate the tracking of law-abiding citizens in their daily lives?

Security experts, editorial writers, think tank operatives and others agree that the Real ID will be used for more and other purposes beyond its originally stated purpose. Schneier in his testimony to the Senate Committee on the Judiciary (2007) raised the issue of the commercial databases which will add Real ID culled information or spring up around Real ID information. So every time the Real ID is swiped, which will be often, the information will end go to many places. In many cases, the rhetoric of DHS is an attempt to turn these uses into selling points for adoption. Jim Harper, of the Cato Institute, agreed with and quoted

Anne Collins, Registrar of Motor Vehicles for the State of Massachusetts, as she predicted that uses of the Real ID card will go far beyond the Congressional intent. In the words of Ms. Collins as reported to the Senate Committee on the Judiciary (2007), “If you build it they will come” (p. 174).

One needs only to look to China to see a parallel endpoint which may be of some concern to a society that has grown used to freedom. China has the usual surveillance camera apparatus, in the city of Shenzen, some 20,000 cameras with computerized software to direct the cameras, and a facial recognition backend to track who is out on the street (Klein, 2008).

China’s residency cards issued to residents starting in August 2007 contain a chip, and information, such as the citizen’s name, address, ethnicity/race, work history, police record, medical insurance information and status, landlord’s phone number, educational background and reproductive status. In the future, credit histories, subway travel balances and petty cash allotments will be added. Just like a student ID card at a major university, the users will be able to make small purchases with these national ID cards. Michael Lin of Public Security Technology, the company that makes the cards, said, “If they do not get the permanent card, they cannot live here, they cannot get government benefits, and that is a way for the government to control the population in the future” (Bradsher, 2007).

Some predict for the Real ID card such trivial (compared to safeguarding airplanes from terrorists) uses as keeping track of “club membership, employment, library usage, even health and credit information” (Healey, 2008).

## 4.10. Possible Role of RFID in Future Real ID Implementations

RFID has applications across a variety of products. For tracking uses, an RFID chip has the advantage of holding enough information that each item can have a unique identifier (Strickland & Hunt, 2005). That means that when an RFID tag is read, and it is correlated with the owner of the item tagged, the association can be made between the person and that RFID chip. Whenever the tag is read, the date, time and location of that encounter can be logged into a database. If an individual has multiple items with RFID tags, the tag can be associated with an individual with a high degree of certainty. These encounters can then be used to track the individual's movements. The individual could be identified by identifying the tags in any subset of the items the person owns.

There is also the concern that there will be a requirement to tag humans with RFID. Chips have been implanted in pets and livestock for years. The company CityWatcher.com, a video surveillance company in Cincinnati requires as a condition of employment that its workers have an RFID chip implanted (Williams, 2007).

A Wisconsin law banning forced implantation of RFID chips in people took effect in June 2006 (Songini, 2006). North Dakota passed a similar law in 2007. (Songini, 2007). The California Senate passed a bill in 2007 banning employers from requiring that employees have chips implanted. The law took effect January 1, 2008 ("California RFID," 2007; del Barco, 2008).

# CHAPTER 5. THE REAL ID ACT AND THE THREAT TO FREEDOM

The Real ID Act in its currently envisioned form is a threat to privacy and freedom in American society. The cost-benefit ratio in the implementation of the act, even in a perfect implementation under the current rules, is poor and is outweighed by the good the money spent on implementation could do if spent on more effective surveillance. More effective surveillance might consist of surveillance of individuals who were indicated by other intelligence to possibly be terrorists, as opposed to surveillance of all American citizens on the chance that one of them might turn into a terrorist without exhibiting other indications of terrorist inclinations. The current rules themselves are a less than perfect implementation of the intent of the Act. Even if DHS mandated a more secure implementation, the insecurities inherent in the sprawling computer system the web of databases represents, would be impossible to implement securely. And a less than perfect implementation of a more secure specification would still be insecure.

Adding to the problems of this type of system is the panoply of threats that are faced by all computer networks and database systems. These include malware of all types, unauthorized access and insider abuse.

## 5.1. Insecurities in the Current Implementation

The information on the cards can be read by any 2D barcode scanner. These types of scanners will be employed in all manner of business to read the cards as they are presented and populate innumerable databases, each operated by some type of commercial entity. These commercial databases are a separate

problem from the security at the state level of the driver's license issuing agencies.

There is no encryption mandated to protect the data on the cards. There is a mandate that DHS will certify states' IT systems as to the security of the data that gets queried with an authorized use of the card. This is a specious guarantee as there is no oversight or third-party security review, so the public is to trust the federal government as it audits the states' IT systems. Federal agencies have the Government Accountability Office (GAO) audit those agencies every year and every year the results are bad. It would be safe to assume that the states are less adept at securing their systems as they have less expertise.

## 5.2. The Problem of Privacy in a Surveillance Society

The problem of privacy of information about oneself as an American citizen is a problem which can be broken down into two parts. The first has to do with what information the government should be entitled to under the theory of security, and the second has to do with what information commercial interests should be allowed to store, maintain and sell. This includes contentless data such as where an individual is at any given time, or what they are wearing, as well as data with content, such as what an individual says, and to whom they say it.

The second question involves enumerated rights. Speech and assembly are enumerated rights, and it was assumed that in American society, one can travel to speak and assemble. The questions of freedom of assembly and anonymous association are directly tied to tracking technologies, inference tracking as it applies to phone calls, emails and Internet traffic.

To reclaim some sense of privacy of information as the situation is currently constituted may be futile. There is a vast amount of data held in private hands,

and much money is being made from the sale and transfer of the information. Free market advocates might maintain that the best way to keep a company from buying and selling transaction information would be for consumers to not do business with companies that have lax or non-existent privacy policies. Froomkin (2000) advises that individuals not fill out surveys and warranty cards, and that they limit the amount of personal information they hand over to commercial entities when possible (p.1464). However, the inertial effect of the market that exists, and the amount of money involved in the data trade make it unlikely that any wholesale change in the way corporations buy, sell and handle data can be expected to materialize in the direction of more privacy for individuals in the manner in which their data is bought or sold by corporations.

## 5.3. We've Got the Wrong Guy

Getting the wrong guy is something that authorities are loathe to have to admit. There are numerous examples of individuals under the traditional criminal justice construct who are convicted of crimes they didn't commit. These errors, or miscarriages of justice, occurred in the framework of a criminal justice system under which the Fourth Amendment and other procedural safeguards existed, and judicial oversight was accepted as having been exercised. Miranda rights, prohibitions against torture of suspects, due process protections, open courts, an appeals system: these are all constructions assumed to be in place on these occasions in which justice has been misapplied or miscarried.

In the world of secret courts with secret evidence and predictive data mining to identify those who might be terrorists in the future, intuitively, the implications are fairly serious in cases in which data is misapplied or the wrong individual is flagged for scrutiny. Without the Constitutional protections afforded by the rule of law and with secrecy implied, any mistakes might never be identified nor rectified.

It is easy to hypothesize examples in which the wrong individual could be implicated by remote tracking surveillance. Consider a crime where the neighbor's teenager had a copy of the victim's car key. The teenager has this key from a time when he ran an errand for the family and had the key copied. The teenager drives late at night with his friends to a deserted place near a power plant to use drugs and drink. Let's suppose that the victim's work cell phone had been left in the car. The tracking computer will see the personal phones at the car owner's house, but all the other tracking surveillance markers will indicate that the worker was nefariously casing the power plant. These markers would include highway RFID readers identifying the RFID chips in the car's tires along the highway, the OnStar records of GPS positioning, and the work cell phone locational tracking records. If anything untoward were to happen at the plant, which is considered critical infrastructure by definition, and even possibly if not, that joyride might bring the police to the victim's house. At that point, the victim would hope that the teenager had brought a cell phone on that ride also.

Similar situations could occur due to the confluence of external events with the mis-identified person talking to the "wrong" person, surfing to the wrong Web site, ordering the wrong thing, going to the wrong series of strip malls in a certain order (let's say that the malls have a rocketry store, a store with chemistry sets, and a UPS Store). If one watched the "wrong" shows on television or read the "wrong" books, one might come under increased scrutiny. Most of the time, there would be little follow-up. Ideally, the national security apparatus would verify that the person was not a threat to the government and then leave them alone.

During the manhunt for the D.C. sniper, Hank Asher used his Matrix system to attempt to identify the sniper based on the victims' residences, attempting to find some commonality to tie the murders together to help solve the crime. Asher rejected the government's theory that the sniper was ex-military, and tried his

own theory, figuring the sniper had geographical ties to the area. By using his Matrix system, Asher came up with the name of a man:

> "So I ran a profile of the distance of every one of the murders, and I came up with a guy that lived like a hundred feet from one of them, five hundred feet from another, two thousand feet from another. I mean, the glove fit," he [Asher] said. "And I sent that up to them [law enforcement] and I can't imagine what that poor fellow…"
>
> "Hopefully he was cleared easily with alibis and excuses," he said. "But I thought I had caught him." (O'Harrow, 2005, p.118)

There have been situations in which NSA passed along useless intelligence to the FBI. During a period of illegal, warrantless wiretapping, the NSA was developing leads for the FBI. These leads were the raw intelligence of phone numbers with which possibly suspicious people had had communication. Specifically mentioned as being passed from NSA to FBI were phone numbers of babysitters and local pizza parlors, numbers of non-co-conspirators. One FBI official said, "After you get a thousand numbers and not one is turning up anything, you get some frustration" (Bamford, 2008, p. 267). Diverting resources in this manner, to following up leads of dubious quality based on the mere fact of a phone call having been made, is a poor use of resources if the goal is anti-terrorism.

The obvious problems arise from the mis-identification and mis-classification of American citizens in these national security and law enforcement databases. O'Harrow (2005) relates the story of Stephan Nash and the Denver police. Mr. Nash was active in an organization named CopWatch, which attempted to expose police brutality and lawlessness with regard to dealings with minorities in the city of Denver. He was also an activist in other legitimate political organizations. It was only through an insider passing on information to Nash and the ACLU that the domestic spying activities of the Denver police came to light.

The Denver police had been spying on civilians for years and the records were paper-based. In 2000, the city wanted to upgrade to computerized databases,

and contracted with Orion Scientific, a company that took software developed by the Defense Advanced Research Projects Agency (DARPA) and extended it for use by domestic intelligence agencies.

What the city of Denver did not do was invest in training. Supervisors were allowed to make up the rules for categorizing the subjects of surveillance as the data was entered. The easiest category to put many of the spied upon was “criminal extremist.” Mr. Nash and his wife were so labeled, as well as an elderly nun who worked with the poor Indians in Chiapas and a Colorado University professor who spoke at a rally against police brutality (O'Harrow, 2005, pp. 274-277)

Meanwhile, these actual and potential abuses are minimized by law enforcement, policy makers and the media as an adjunct of the government. The current reportage treats privacy abuses as unusual, portraying these as man bites dog stories. The prevailing frame is always, “If it saves even one life, then it is worth it.” In acquiescing to the government’s declaration of extraordinary powers and suspension of habeas corpus in general and for American citizens as “enemy combatants” (Levy, 2003; “Jose Padilla,” n.d.) and allowing the creation of a separate legal system (“Military Commissions Act of 2006,” 2006; “ACLU: Military Commissions Act of 2006,” n.d.), citizens have demonstrated acceptance of this abuse. American society moved away from the Founding Fathers’ guiding principle of jurisprudence, which is credited to William Blackstone, that of “innocent until proven guilty.” In the famous quote, “Better that ten guilty persons escape than that one innocent suffer” (Volokh, 1997, p.174; Blackstone, 1893, p. *358) is found the abhorrence of arbitrary detention and show trials with rigged verdicts that the American Revolutionaries rejected in their bid for freedom from the King’s and his functionaries’ whims and fairness in the legal process. The lack of substantive debate in the mainstream media and the framing of mainstream media coverage regarding this radical shift in American public policy

in the legal realm is consistent with the Propaganda Model as advanced by Herman and Chomsky (1988).

## 5.4. Abuse of Trust

All of the data in one place--that is the scenario that evildoers like to see. That is the essence of one-stop shopping. That is what the Real ID distributed database will be. Sometimes the evildoers are seemingly trustworthy individuals. The three letter agencies also seem to have trouble identifying who might be a security risk and who is not a risk.

Nada Nadim Prouty, 37, who started life in Lebanon, was a former employee of the FBI and CIA. In November, 2007, she pleaded guilty to conspiracy to defraud the U.S. government. She allegedly fraudulently acquired U.S. citizenship, and then is said to have used her position at the FBI to access data about family members who are alleged to have connections to Hezbollah.

Prouty entered the U.S. from Lebanon in June 1989 on a non-immigrant student visa, stayed past the expiration of her visa, and then paid a U.S. citizen to marry her on August 9, 1990. In April 1999, she was hired as a special agent of the FBI, was granted a security clearance and worked out of the Washington field office investigating crimes against U.S. persons overseas.

In August 2000, Prouty's sister married Talal Khalil Chahine. Chahine is now a fugitive hiding out in Lebanon, according to DOJ and is wanted in connection with tax evasion in the matter of a concealed $20 million, some of which was diverted to Lebanon.

In June 2003, before leaving the FBI to join the CIA, Prouty accessed the FBI's Automated Case System and queried her name, her sister's name, and that of

Chahine. She resigned the CIA in November 2007 and offered to help the CIA on matters involving national security (Gross, 2007).

The conclusion that can be drawn is in two parts. In the first part, it is obvious that organizations which are supposed to be good at screening their applicants end up letting individuals into the organization with questionable ties. Once in the organization, an individual like Prouty can access sensitive information. The implication for the Real ID data is that in organizations with less rigorous screening, such as police departments, there is a greater likelihood that people who should not be trusted with American citizens' data will be. The second component involves the inherent insecurity of the data to insider abuse in general.

## 5.5. Abuse of Power

An audit of 10 percent of the FBI's national security investigations since 2002 revealed that the FBI had violated the law or agency rules on more than 1,000 occasions. The sample size and the numbers indicate that the FBI had illegally collected information several thousand times. The majority of the incidents involve phone companies and Internet Service Providers (ISPs) furnishing information the agents were not authorized to collect (J. Solomon, 2007).

A report issued in March of 2007 by the Justice Department did not uncover the extent of the illegality revealed in June, but did include Attorney General Gonzalez and FBI Director Robert S. Mueller admitting that the FBI broke the law in collecting information improperly under the PATRIOT Act. The Attorney General even left the door open to the possibility of pursuing criminal charges against FBI agents and lawyers who broke the law (Jordan, 2007).

There are numerous instances of police and various others who have accessed law enforcement databases with citizens' personal data in an unauthorized fashion ("If you have nothing…", 2008). One instance involved Officer Theresa Shover of the DeKalb County Police Department accessing the Georgia Crime Information Center database, a database that is supposed to be classified, to get information on her ex-husband's girlfriend. She then created flyers with the ex-husband's girlfriend's picture and captions labeling her an adulteress, homewrecker, etc., and sent these to the woman's family, friends, past employer, et al., with social networking information gained from the database. More astonishing was the fact that she was suspended and not charged criminally ("Officer suspended," 2008).

## 5.6. Insecurity of Information and the Power of the Database

There are instances in which sensitive and even classified information is not secure. This augurs poorly for the security of the Real ID database.

One instance of sensitive information being exposed on the Web comes from the architects commissioned to design the U.S. Embassy in Baghdad. Berger Devine Yaeger Inc. of Kansas City exposed the master drawings for the embassy, which will sit on 104 acres in Baghdad, on its Web site in May, 2007.

The State Department asked the firm to remove the drawings from their site. After that request had been issued, a spokesman for the company said that anyone who was interested could just look the site up on Google Earth.

Al Jazeera had reported bombings of construction equipment and that construction personnel had been injured. With the drawings and the Google Earth information, however, it would be an easy job to match the construction phases with the observed activity (Jones, 2007).

Even beyond information that is sitting in databases that can be accessed from many points by many entities, such as that which the Real ID distributed database represents, there are problems securing data in supposedly the most secure environments. In 2007, various problems surfaced at Los Alamos, including the leaking of classified data over the Internet, a laptop with sensitive documents stolen from a vacationing staffer in Ireland, and the transmission of unencrypted information through email (Barry, 2007).

## 5.7. Government is not the Solution, Government is the Problem

There may be some ways in which the data and privacy problems can be addressed. Vehicle registration information is kept precisely and even pre-9/11 was made available in the aggregate to various industry and trade groups ("U.S. automobile registrations," 2001). There is no compelling need to ship raw data which would link individuals to the data elements in various databases to commercial and governmental entities. The data should be aggregated as a way to anonymize data.

There should be encryption used for the data being written to and read from the Real ID cards. The databases should have the data in them encrypted. The federal government is moving toward whole disk encryption since the VA data loss affair. Every Web browser has encryption built in for credit card transactions, among others. There is a system of certificates so that entities can be verified as to their identity against the certificate authority's certificate. Some certificates use a cryptographic algorithm, MD-5, which has exhibited weakness, and which allows forgers to create fake certificates (MD5 Weakness Allows Fake SSL Certificates To Be Created, 2008). The problems with MD-5 are solvable, in that certificate authorities (CAs) can use a more secure algorithm such as SHA-1 and therefore a fairly secure certificate implementation can be achieved. When

vulnerabilities are discovered in SHA-1 are discovered, then another more secure algorithm will have been developed.

States have been selling their citizens' personal data to data aggregators for years. An example of this practice is the state of Minnesota, which sold driver's license information to over 5,000 outside groups. Attorney General Mike Hatch noted that, "The name, address, height, weight and driver's license number of every Minnesota driver can be accessed over the Internet by anyone willing to pay for it. If you don't thank that's shocking, the threat is brought to you by state government." (Scheck, 2006, par. 3)

There are situations in database inquiries, in which database queries can be constructed to destroy privacy, and there is active research in the computer science community into ways to guard against those types of series of database queries which would reveal information which should remain private.

## 5.8. Conclusions

The net effect of total surveillance serves to chill individual freedom and expression, thereby enforcing conformity and denying the benefits of participatory democracy. The Hawthorne effect was observed by Elton Mayo at the Western Electric Hawthorne plant in Illinois in a series of experiments on worker productivity. Although Jones (1992) conducted a reexamination of the original study, it is still conventionally accepted that people behave differently when observed. Jeremy Bentham's Panopticon, which revolutionized architectural and organizational design of prisons, factories, schools and orphanages, was based on the idea that control could be achieved by watching those who were to be controlled without the observed knowing whether or not they were being observed. This tended to make the subject population believe they were under surveillance at all times. Froomkin (2000) describes this effect in

passing (p. 1463) as a privacy issue. Strub (1989) takes this theme further, reading Orwell's 1984 through Bentham and arriving at a disconcerting end.

With the FBI and law enforcement agencies now free to infiltrate peaceful social justice and groups expressing legitimate political dissent, the chilling effect of suppression of citizens' voices in the political process is inevitable (Johnson, 2008; Madigan, 2008). When anonymity of association is deprived, people cannot join and support causes that align with their policy and political views. That was the point of Justice Douglass' opinion in *Laird v. Tatum*. People act differently and make decisions differently when they believe they might be watched. In Bamford's (2008) discussion of the Aquaint computer he notes, "Such a system would have an enormous chilling effect on everyone's everyday activities--what will the Aquaint computer think if I buy this book…" (p.327).

And that is the point. In Mexico, legitimate political figures are wiretapped and surveilled at all times. Guanajuato state governor Vicente Fox, later president of Mexico, had his phones tapped. An opposition Senator had seven years of his life recorded in wiretaps and physical surveillance (Bamford, 2008). "The system the Bush administration wanted for Mexico was similar to its warrantless eavesdropping operation in the U.S." (Bamford, 2008, p.227).

When a person has to think twice before saying something, because the unseen monitors are listening; when people are afraid to buy a book because they might get flagged in a database as a subversive; when people are afraid to go get a cup of coffee at a coffee shop because musicians might be singing about something not perfectly aligned with government policy; one could say they are observing the hallmarks of an unfree society, maybe something along the lines of East Germany or the Soviet Union under communism, or China today. There are those that would go so far as to say the type of society being described in a total surveillance regime is Orwellian (Strub, 1989).

There are also those who expound the virtues of conducting surveillance against all of the citizens all of the time. There are advantages associated with total surveillance. Crime might be reduced significantly. Missing people would not be missing for long. No illegal alien or unregistered car would exist within the boundaries of the surveillance perimeter. There would be no object for which an accounting could not be made. No copyrighted work would be used without the proper royalties being credited. And of course, the purpose given for the surveillance would be completely and actually achieved, terrorists would never be able to plot their evil deeds, nor carry them out, or when they did, their associates would be hunted down expeditiously.

The average citizen may have little to fear at present because the government is awash in data and cannot possibly process all of the data on every citizen all of the time. This puts the threat to the average citizen as a “potential” threat to freedom, as opposed to an “actual” threat to freedom. If that is the case, only when someone makes the wrong move and gets on a list, the all-seeing eye of the state will then be trained on that individual. The No-Fly List is a perfect example. The No-Fly List has a million names representing approximately 400,000 people (obviously each terrorist has on average 2.5 names). Many Americans are on that list when they should not be. Wolf (2007) contends that the list is a way to inconvenience individuals who disagree with administration policies (p. 95). She hypothesizes that that is why she and Ted Kennedy are on the list. Others on the list cannot even remotely be considered a terrorist treat.

In other cases, the power of databases over people’s lives when a mistake is made can be considerable. In some of the cases of mistaken identity, there is no recourse for the party who was harmed. O’Harrow (2005) relates the story of the widow of a senior Postal Service executive. She was born to the son of a slave, and as a child she took cover on the floor of her father’s business from gunmen angry at the fact that black aviators were allowed to fly in combat in World War II.

Routinely the TSA would make the same “mistake” over and over. Every time she flew, she was detained until minutes before her flight. Then she would have to run to make the flight. Repeated letter writing and other attempts at remedies, including a letter from the FBI saying she was not a terrorist, did not help the matter. TSA workers ignored the FBI letter and she was told there was no recourse in that she would never get off the list (pp.230-231).

As the Real ID is used to track American citizens who have committed no crime, writing their daily activities into databases, there are more chances for an innocent person to do something that will trigger an investigation. There are more chances for “mistakes.” As the processing power of the computers analyzing the data grows, more people will be flagged. And more “mistakes” will be made. The surveillance apparatus will be fed with data from the tracking of law-abiding American citizens swiping their insecure, unencrypted Real ID at the health club, the airport, the doctor’s office, the library, the clothing store (to make sure they are who their credit card says they are) and the supermarket.

## 5.9. The Rhetoric of the Global War on Terror

The United States has set out in its long-term goals for combating terrorism the ideal of “freedom and dignity that comes when human liberty is protected by effective democratic institutions” (*National strategy*, 2006, p. 1). Later in the statement, the USA PATRIOT Act is held up as a reform that promotes security while “also protecting our fundamental liberties” (p.4). In the long-term approach section of the strategy for winning the war on terror, the long-term goal is stated as “Advancing effective democracy.”

The rhetoric in the National Strategy for Combating Terrorism for fighting the Global War on Terror is replete with references to the concept of participatory democracy for other countries. “But elections are not enough. Effective

democracies… are responsive to their citizens, submitting to the will of the people" (*National strategy*, 2006, p. 9). Yet the reality regarding the Real ID Act, which has been opposed by as many as 38 states at one time, indicates that the federal government will try to do what it will, regardless of the citizens' wishes.

There should have been made here a case that Real ID will not lead to greater security in cases of attempting to protect the public and the state from the truly bad people, the "evildoers" as President Bush characterized them. The idea is flawed, but the implementation is further flawed. In the words of Bruce Schneier, it is "security theater" (Schneier, 2007). And, as Schneier also noted in his testimony to the Senate, it is a "lousy security trade-off," which will cost at least $20 billion and the taxpayer "won't get much security in return" (*Real ID Act Hearings*, 2007, p. 237). Also, it must be assumed that knowledgeable people understand that this bit of security theater is not effective when the public isn't buying it. Yet there must be a reason that DHS and those who are pushing this idea are pushing so hard. There can only be two possibilities, or a combination of the two.

Either the stakes in contractual arrangements are so high, and there is so much money to be made, that the call of profits greatly outweigh the public interest, or the secondary uses of the technology are actually primary. In understanding the believability of the rhetoric of DHS, one must consider that the agency pushing this on the American public, and the Mexican and Canadian public, and then the world public, had on their payroll an individual who staged a fake news conference. FEMA convened a "news conference" about the California wildfires that was carried on some cable channels. FEMA announced the staged event 15 minutes before it was to start, and real reporters could dial in to listen but not ask questions. The individuals in the room who were asking the questions were FEMA employees posing as reporters. The day it happened was one of the last days on the job for the FEMA director of external affairs, John "Pat" Philbin. Mr.

Philbin moved on to his new post as head of public affairs at the Office of the Director of National Intelligence (Hsu, 2007a).

Great Britain is in a similar situation vis-à-vis the Global War on Terror. It has been struck by terrorism, most notably in the attack on the London subway system. The British Intelligence-Led Policing model has been adopted by the United States. Law enforcement wants the surveillance abilities that Britain's national network of closed circuit TV cameras represents. Yet Sir Ken Macdonald, who left his post as Director of Public Prosecutions, made the statement that "the expansion of technology by the state into everyday life could create a world future generations 'can't bear'" (Hope, 2008, par. 1). Sir Ken warned about the "Big Brother" state. He also warned Members of Parliament:

> It is in the nature of State power that decisions taken in the next few months and years about how the State may use these powers, and to what extent, are likely to be irreversible. They will be with us forever. And they in turn will be built upon. So we should take very great care to imagine the world we are creating before we build it. We might end up living with something we can't bear. (Hope, 2008, par. 15-16)

Bamford's (2008) book concludes with the following warning:

> More than three decades ago, when the NSA posed a fraction of the privacy threat it poses today with the Internet, Digital communications, and mass storage, Senator Frank Church, the first chairman of the Senate Intelligence Committee, investigated the NSA and issued a stark warning:
>
> > That capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology.
>
> There is now the capacity to make tyranny total in America. Only law ensures that we never fall into that abyss--the abyss from which there is no return. (pp. 344-345)

## 5.10. Epilogue

Joe and Jane Doe read some of the books listed in the reference section of this work. They paid with cash, thinking it would raise one less flag in the national database, although they knew that if an investigator were to investigate the identities of individuals who might have purchased various books, the digital camera feed, keyed to the bar code scanner entries for the book purchases, would give them away. The investigator could get the pictures, sound and cash register data without ever leaving the Office of National Intelligence as it would be sent over the Internet. They could have borrowed the book from the library, but they would have had to produce a library card and be tied to the book that way, and then their fingerprints would be in one more place--on the pages of the books. “Proof” that they read the books.

They wondered if the video-conferencing capability on the HDTV was turned on and maybe someone or some computer was watching and recording them. Not wanting to take a chance, they went into the bathroom and ran the water in the sink before they had a discussion. They discussed possibly joining some type of privacy group online, but decided against it because they were afraid that might trigger a flag in the national database. They discussed whether they should join a privacy or social action group that had actual meetings, but decided against it because they were afraid they might be put into the database as criminal extremists by government watchers. They debated writing a letter to the newspaper but signing the letter with a fake name. Using their real names might trigger a red flag in the national intelligence database. That sounded ok until they realized that if it triggered a red flag in the national intelligence database and the letter had no fingerprints, or if the name didn’t check out, then it would be worse, especially when the secret dots on the paper tying their printer to the printed copy would give them away. Then they decided that based on what they knew from Herman and Chomsky, that it probably wouldn’t be published anyway.

They decided that their safest option would be to do nothing. They turned the water off and went back to sitting in front of the HDTV, just in case it was watching them. Then it would see that they were doing nothing of a terroristic nature. They watched as the HDTV and databases served targeted advertisements to them. In their minds they reviewed their actions during the day, sure they did nothing that would trigger a red flag in the national database

# LIST OF REFERENCES

# LIST OF REFERENCES

9/11_Commission. (2004). *The 9/11 Commission report*. Washington, D.C.: 9/11 Commission.

49 C.F.R. Part 1520 - Protection of sensitive security information. (2004, May 18). *Code of Federal Regulations*. Retrieved December 27, 2008, from http://law.justia.com/us/cfr/title49/49-9.1.3.4.7.html

AAMVA card design specifications: FAQs. (2008). *American Association of Motor Vehicle Administrators*. Retrieved December 27, 2008, from http://www.aamva.org/KnowledgeCenter/Standards/Current/DLIDSpecificationFAQs.htm

Abdul-Alim, J. (2000, October 22). Racine sailor details attack. *Milwaukee Journal Sentinel*. Retrieved October 5, 2008, from http://www.jsonline.com/news/metro/oct00/cole23102200a.asp

Abele, R. (2005). *A user's guide to the USA PATRIOT Act and beyond*. Lanham, Maryland: University Press of America, Inc.

Abelson, J. (2007). Breach of data at TJX called the biggest ever. *Boston Globe*. Retrieved from http://www.boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/

About smart cards: Applications: Transportation. (2009). *Smart Card Alliance*. Retrieved January 6, 2009, from http://www.smartcardalliance.org/pages/smart-cards-applications-transportation

ACLU: Military Commissions Act of 2006. (n.d.). *American Civil Liberties Union*. Retrieved February 22, 2009, from http://www.aclu.org/safefree/detention/commissions.html

An Act Concerning Aliens, (1798).

Avery, S. (2008). Patriot Act haunts Google service. Retrieved August 31, 2008, from http://www.theglobeandmail.com/servlet/story/RTGAM.20080324.wrgoogle24/BNStory/Technology/?cid=al_gam_nletter_dtechal

Badey, T. (1998). Defining international terrorism: A pragmatic approach. *Terrorism and Political Violence*, 10(1), 90-107.

Bamford, J. (2008). *The shadow factory*. New York: Doubleday.

*Bank Secrecy Act: FinCEN and IRS need to improve and better coordinate compliance and data management efforts*. (2006). Washington, D.C.: Government Accountability Office.

Barrett, C. (2002). FBI Internet surveillance: The need for a natural rights application of the Fourth Amendment to insure Internet privacy. *Richmond Journal of Law and Technology*, *8*(Spring).

Barry, J. (2007, June 25). Lax and lazy at Los Alamos. *Newsweek*. Retrieved July 4, 2007, from http://www.msnbc.msn.com/id/19418769/site/newsweek/page/0

Behar, R. (2004, February 23). Never heard of Acxiom? Chances are it's heard of you. *Fortune*. Retrieved November 7, 2008, from http://money.cnn.com/magazines/fortune/fortune_archive/2004/02/23/362182/index

Bennett, M. (1966). The Immigration and Nationality (McCarran-Walter) Act of 1952, as amended to 1965. The ANNALS of the American Academy of Political and Social Science, 367(1).

Berman, J., & Mulligan, D. (1999). The Internet and the law: Privacy in the digital age: Work in progress. Nova Law Review, 23(Winter).

Bhattacharya, I., & Getoor, L. (2007). Collective entity resolution in relational data. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1).

Bill of Rights. (1791). Washington, D.C.: Library of Congress.

Big bucks: Billions for surveillance (2008, October 4). Retrieved February 15, 2009, from http://www.videosurveillanceguide.com/articles/big-bucks-billions-for-surveillance.htm

Binkley, C. (2004, November 22). Numbers game: Taking retailers' cues, Harrah's taps into science of gambling; others focus on high rollers while casino giant prefers telemarketing, databases; from East Chicago to Caesars. Wall Street Journal. Retrieved January 9, 2009, from http://www2.lib.purdue.edu:2118/pqdweb?index=0&did=740619091&srchmode=2&sid=1&fmt=3&vinst=prod&vtype=pqd&rqt=309&vname=pqd&ts=1231555367&clientid=31343

Blackstone, W. (1893). Book the fourth. Of public wrongs. In G. Sharswood (Ed.), Commentaries on the laws of England in four books. notes selected from the editions of Archibald, Christian, Coleridge, Chitty, Stewart, Kerr, and others, Barron Field's analysis, and additional notes, and a life of the author. Philadelphia: J.B. Lippincott Co.

Bloss, W. (2008). Escalating U.S. police surveillance after 9/11: An examination of causes and effects. Surveillance and Society, 4(3), 208-228.

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the Internet: Self-Regulation or government regulation? Business Ethics Quarterly, 16(3), 323-342.

Bradsher, K. (2007, August 12). China enacting high-tech plan to track people. New York Times, from http://www2.lib.purdue.edu:6624/purdue?url_ver=Z39.88-2004&url_ctx_fmt=infofi/fmt:kev:mtx:ctx&ctx_enc=info:ofi/enc:UTF8&ctx_ver=Z39.882004&rfr_id=info:sid/sfxit.com:azlist&sfx.ignore_date_threshold=1&rft.object_id=110975413976006

Branum, T. (2001). Aviation security in the new century: Federalist Society for Law & Public  Policy Studies.

Bremmer, C. (2008, September 9). French revolt over Edvige: Nicolas Sarkozy's big brother spy computer. TimesOnline. Retrieved December 31, 2008, from http://www.timesonline.co.uk/tol/news/world/europe/article4703054.ece

Brownlee, N., & Claffy, k. (2004). Internet measurement. Internet Computing: IEEE, 8(5), 30-33.

Bumiller, E., & Stevenson, R. (2004, August 31). The Republicans: The convention in New York -- The President; Bush cites doubt America can win war on terror New York Times. Retrieved January 10, 2009, from http://query.nytimes.com/gst/fullpage.html?res=9b02e4df1431f932a0575bc0a9629c8b63&sec=&spon=&pagewanted=print

Burke, J. (2004). Al Qaeda. Foreign Policy(142), 18-20+22+24+26.

Bush, G. (2003, December 13, 2003). Statement on H.R. 2417. Office of the Press Secretary. Retrieved November 18, 2007, from http://www.whitehouse.gov/news/releases/2003/12/20031213-3.html

Bush, G. (2005, May 11). President's Statement on H.R. 1268. Retrieved December 19, 2008, from http://www.whitehouse.gov/news/releases/2005/05/print/20050511-6.html

Bush, G. (2008, February 29). Executive Order: President's Intelligence Advisory Board and Intelligence Oversight Board. The White House. Retrieved December 31, 2008, from http://www.whitehouse.gov/news/releases/2008/02/20080229-5.html

Bush, G. W. (2001). Address to a Joint Session of Congress and the American people. Retrieved November 17, 2008, from http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html

Caldwell, P. (2006). GPS technology in cellular telephones: Does Florida's Constitutional privacy protect against electronic locating devices? Journal of Technology Law & Policy, 11(June).

California RFID bill signed into law today by Governor. (2007). ACLU of Northern California. Retrieved January 4, 2009, from http://www.aclunc.org/issues/TECHNOLOGY/blog/california_rfid_bill_signed_into_law_today_by_governor.shtml

Cangeloso, S. (2008, September 30). RFID tag anything with Tikitag. Geeks.com. Retrieved January 11, 2009, from http://www.geek.com/articles/chips/rfid-tag-anything-with-tikitag-20080930/

Carr, R. K. (1951). The Un-American Activities Committee. The University of Chicago Law Review, 18(3).

Case 3:07-cv-00109-VRW - Document 71. (2009, February 13). United States District Court for the Northern District of California. Retrieved February 15, 2009, from http://www.eff.org/files/filenode/att/alharamainorder21309.pdf

Cassese, A. (2006). The multifaceted notion of terrorism in international law. Journal of International Criminal Justice, 4(5), 933-958.

The cell phone challenge to survey research. (2006, May 15). Pew Research Center. Retrieved January 11, 2009, from http://peoplepress.org/report/276/

Charny, B. (2004, September 29). Janet Jackson still holds TiVo title. Retrieved January 7, 2009, from http://news.cnet.com/janet-jackson-still-holds-tivo-title/2100-1041_3-5388626.html

Chertoff, M. (2006a). Remarks by Secretary of Homeland Security Michael Chertoff on September 11: Five Years Later. Retrieved June 8, 2008, from http://www.dhs.gov/xnews/speeches/sp_1158335789871.shtm

Chertoff, M. (2006b, December 13, 2006). Remarks by Secretary of Homeland Security Michael Chertoff, Immigration and Customs Enforcement Assistant Secretary Julie Myers, and Federal Trade Commission Chairman Deborah Platt Majoras at a press conference on Operation Wagon Train. Retrieved April 24, 2008, from http://ww.dhs.gov/xnews/releases/pr_1166047951514.shtm

Chertoff, M. (2008a, January 16). Michael Chertoff: National ID security. Retrieved December 20, 2008, from http://www.sacbee.com/opinion/v-print/story/636479.html

Chertoff, M. (2008b, January 11). Remarks by Homeland Security Secretary Michael Chertoff at a press conference on Real ID. Retrieved December 25, 2008, from http://www.dhs.gov/xnews/speeches/sp_1200320940276.shtm

Chomsky, N., & Matta, W. (2008, August 1). Untitled interview: Noam Chomsky interviewed by Wissam Matta, Assafir newspaper (Lebanon). Retrieved January 10, 2009, from www.chomsky.info/interviews/20080801.htm

A chronology of data breaches. (2009, January 6). Privacy Rights Clearinghouse. Retrieved January 11, 2009, from http://www.privacyrights.org/ar/ChronDataBreaches.htm

Clerk's notice in Al-Haramain Islamic Foundation, Inc. et. al. v. George W. Bush et. al. (2009, January 6). United States District Court for the Northern District of California. Retrieved January 10, 2009, from http://www.eff.org/files/filenode/att/alharamaincmc010609.pdf

Cole, D., & Dempsey, J. (2002). Terrorism and the Constitution. New York: The New Press.

Cole, E. (2003). Hiding in plain sight :Steganography and the art of covert communication. New York: Wiley Pub.

Congressman Sensenbrenner. Retrieved December 21, 2008 from http://sensenbrenner.house.gov/Biography/

Coombes, A. (2008, August 20). IRS employee sentenced for snooping. MarketWatch. Retrieved January 3, 2009, from http://www.marketwatch.com/news/story/irs-worker-snooped-tax-records/story.aspx?guid=%7b786bacbd-c58f-481b-ae31-28c2101e7cf6%7d

Countryman, A. (2003, December 28). Illegal insider trading detection takes digging, sophisticated surveillance. Knight Ridder Tribune Business News. Retrieved January 9, 2009, from http://www2.lib.purdue.edu:2118/pqdweb?index=14&did=515929531&srchmode=1&sid=2&fmt=3&vinst=prod&vtype=pqd&rqt=309&vname=pqd&ts=1231555902&clientid=31343

Crenshaw, M. (2001). Why America? The globalization of civil war. Current History, 100(650), 425-432.

Date, C. J. (1995). An Introduction to database systems (6th ed.). New York: Addison-Wesley Publishing Company, Inc.

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: public opinion in the context of the terrorist attacks on America. American Journal of Political Science, 48(1), 28-46.

del Barco, M. (2008, January 1). California law outlaws RFID implant mandate. National Public Radio. Retrieved February 29, 2009, from http://www.npr.org/templates/story/story.php?storyId=17762244

Deleting Web browser cookies & cache. (2006, August 31). New York University Information Technology Services. Retrieved January 7, 2009, from http://www.nyu.edu/its/faq/cache.html

Devita-Raeburn, E. (2008). If there's really only six degrees (of separation) between us and Osama bin Laden, why can't we find him? Discover, 29(2), 42-46.

DHS Basic Pilot /E-Verify Program. (2008, March). National Immigration Law Center. Retrieved February 21, 2009, from http://www.nilc.org/immsemplymnt/ircaempverif/e-verify_infobrief_2008-03-13.pdf

Digital recording with Dibos in bank applications. (2004, March 3). Bosch. Retrieved January 9, 2009, from http://resource.boschsecurity.com/documents/DiBos19InchDigi_ApplicationReference_Bank_enUS_T2822415627.pdf

Ditzion, R. (2004). Electronic surveillance in the Internet age: The strange case of pen registers. American Criminal Law Review, 41(Summer).

Dixon, R. (1997). Windows nine-to-five: Smyth v. Pillsbury and the scope of an employee's right of privacy in employer communications. Virginia Journal of Law and Technology, 2(Fall).

Doran, M. (2002). The pragmatic fanaticism of al Qaeda: An anatomy of extremism in Middle Eastern Politics. Political Science Quarterly, 117(2), 177-190.

Dunham, R. S. (2005). The PATRIOT Act: Business balks. Business Week. Retrieved from http://www.businessweek.com/bwdaily/dnflash/nov2005/nf20051110_9709_db016.htm

E-Z Pass toll system. (2006, January 18). Import Rival Site. Retrieved January 7, 2009, from http://www.importrival.com/modules/AMS/article.php?storyid=37

EFF analysis of 'PATRIOT II'. (n.d.). Electronic Freedom Foundation. Retrieved November 18, 2007, from http://w2.eff.org/censorship/terrorism_militias/patriot-act-ii-analysis.php

Eggen, D. (2006, January 28, 2006). 2003 draft legislation covered eavesdropping. Washington Post. Retrieved November 18, 2007, from http://www.washingtonpost.com/wpdyn/content/article/2006/01/27/ar2006012701476.html

Elias, P. (2007, August 6). Secret call log at heart of wiretap challenge. USA Today. Retrieved January 10, 2009, from http://www.usatoday.com/tech/news/surveillance/2007-08-05-thedocument_n.htm?csp=34

Elmore, M. (2001). Big Brother where art thou? Electronic surveillance and the Internet: Carving away Fourth Amendment privacy protections. Texas Tech Law Review, 32.

Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005. (2005).

Eureste, M. A. (2008, December 18). Steps to avoid violating employee privacy rights. HR Tools. Retrieved January 9, 2009, from http://www.hrtools.com/insights/mary_alice_eureste/steps_to_avoid_violating_employee_privacy_rights.aspx

Ezovski, G. M., & Watkins, S. E. (2007). The electronic passport and the future of government-issued RFID-based identification. Proceedings of IEEE International Conference on RFID, 2007, 15-22.

Ferguson, R. B. (2007, February 28). DHS confirms Real ID Act regulations coming; States rebel. eWeek. Retrieved October 19, 2008, from http://www.eweek.com/c/a/mobile-and-wireless/dhs-confirms-real-id-act-regulations-coming-states-rebel/

Fishkin, K. P., Jiang, B., Philipose, M., & Roy, S. (2004, June). I sense a disturbance in the Force: unobtrusive detection of interactions with RFID-tagged objects. Ubicomp. Retrieved January 11, 2009, from http://www.seattle.intel-research.net/pubs/062420041544_244.pdf

Florida Constitution. (1968). Florida Senate. Retrieved January 10, 2009, from http://www.flsenate.gov/statutes/index.cfm?mode=constitution&submenu=3&tab=statutes&CFID=120535607&CFTOKEN=21785735#A01S23

Foley, J. (2007). Are Google searches private? An originalist interpretation of the Fourth Amendment in online communication cases. Berkeley Technology Law Journal, 22(Annual Review).

Fox, B. (2006, April 26). Invention: Apple's all-seeing screen. New Scientist. Retrieved November 7, 2008, from http://www.newscientist.com/article.ns?id=dn9059&print=true

Frederickson, S. (2008). Tapping into the reporter's notebook. The News Media the Law, 32(4).

Freiwald, S. (2007). First principles of communications privacy. Stanford Technology Law Review, 2007.

Froomkin, A. (2000). The death of privacy? Stanford Law Review, May, 2000.

Garrett, G. (1919). Free speech and the Espionage Act. Journal of the American Institute of Criminal Law and Criminology, 10(1).

Garrow, D. (1988). FBI political harassment and FBI historiography: Analyzing informants and measuring the effects. The Public Historian, 10(4), 5-18.

German consumers rebel over RFID tracking at METRO Future Store. (2004, February 26). SpyChips. Retrieved January 11, 2009, from http://www.spychips.com/press-releases/german-protest.html

Glancy, D. (1995). Privacy and intelligent transportation technology. Santa Clara Computer and High Technology Law Journal, 11.

Glancy, D. (2000). Symposium on Internet privacy: At the intersection of visible and invisible worlds: United States privacy law and the Internet. Santa Clara Computer and High Technology Law Journal, 16(May).

Glenn, M. (2003). A summary of DoS/DDoS prevention, monitoring and mitigation techniques in a service provider environment: SANS/GSEC.

Godfrey, S. (2008, December 3). Nobody rides for free. Washington City Paper. Retrieved February 22, 2009, from http://www.washingtoncitypaper.com/display.php?id=36563

Goldberg, M. (2005). The Googling of online privacy: Gmail, search-engine histories and the new frontier of protecting private information on the Web. Lewis and Clark Law Review, 9(Spring).

Goldstein, R. (2006). Prelude to McCarthyism: The making of a blacklist. Prologue, 38(3).

Goodin, D. (2009, February 2). Passport RFIDs cloned wholesale by $250 eBay auction spree. The Register. Retrieved February 3, 2009, from http://www.theregister.co.uk/2009/02/02/low_cost_rfid_cloner/

Goodman, A. (2008, September 4). Eight members of RNC activist group lodged with terrorism charges. Democracy Now. Retrieved January 10, 2009, from http://www.democracynow.org/2008/9/4/ eight_members_of_rnc_activist_group

Goodman, A., & Klein, M. (2008, July 7). AT&T whistleblower urges against immunity for telecoms in Bush spy program. Democracy Now. Retrieved January 9, 2009, from http://i4.democracynow.org/2008/7/7 /att_t_whistleblower_urges_against_immunity

Goodman, A., Rosa, E., German, M., & Clancy, E. (2008, August 1). Colorado “Fusion Center” to step up intelligence gathering during DNC; US Northern Command to play role. Democracy Now. Retrieved January 11, 2009, from http://www.democracynow.org/2008/8/1/ colorado_fusion_center_to_step_up

Goodman, A., & Weiser, W. (2006, October 31). Vote suppression in 2006: Rule changes threaten to disenfranchise hundreds of thousands of eligible voters. Democracy Now. Retrieved January 9, 2009, from http://www.democracynow.org/2006/10/31/vote_suppression_in_2006_rule_changes

Gorman, S. (2008, March 10). NSA's domestic spying grows as agencies sweep up data. Wall Street Journal. Retrieved July 28, from http://online.wsj.com/public/article_print/SB120511973377523845.html

Government requests for real time phone location data divide magistrates. (2006). Electronic Commerce & Law Report, 11(2).

GPS vehicle tracking systems. (2008). Enfotrace. Retrieved January 9, 2009, from http://www.enfotrace.com/market/index.html

Graham, N. (2005). Note: PATRIOT Act II and denaturalization: An unconstitutional attempt to revive stripping Americans of their citizenship. Cleveland State Law Review, 52.

Granger, S. (2001, December 18). Social engineering fundamentals, part I: Hacker tactics Security Focus. Retrieved February 20, 2009, from http://www.securityfocus.com/infocus/1527

Greene, T. (2004, October 14). Feds approve human RFID implants. The Register. Retrieved January 10, 2009, from http://www.theregister.co.uk/2004/10/14/human_rfid_implants/print.html

Greenemeier. (2007, July 5). Downed electronic Jihad site flew under the radar. Information Week. Retrieved July 10, 2007, from http://www.informationweek.com/news/showarticle.jhtml?articleid=200900590

Grier, D. A. (2006). The innovation curve. Computer, 39(2), 8-10.

Gritzinger, B. (2008, September 26). Black box on board. Auto Week. Retrieved January 8, 2009, from http://www.autoweek.com/apps/pbcs.dll/article?aid=/20080924/free/809189970/1023/thisweeksissue

Gross, G. (2007). Former FBI, CIA agent pleads guilty to computer crime. Computer World. 2008 (October 26). Retrieved from http://www.computerworld.com/action/article.do?command=printarticlebasic&articleId=9046802

H.R. 418 - THOMAS (Library of Congress). (2005). Retrieved December 20, 2008, from http://thomas.loc.gov/cgi-bin/bdquery/z?d109:hr00418:

Haas, B., & Giovis, J. (2008, May 20). Crime can strike fast at south Florida malls. TCPalm. Retrieved February 15, 2009, from http://www.tcpalm.com/news/2008/may/20/crime-can-strike-fast-south-florida-malls/

Halbert, S. (1958). The suspension of the Writ of Habeas Corpus by President Lincoln. The American Journal of Legal History, 2(2).

Harper, J. (2007). Understanding the realities of Real ID. Vital Speeches of the Day, 73(5), 208-212.

HB 1716. (2008, October 15). Missouri House of Representatives. Retrieved December 24, 2008, from http://www.house.mo.gov/billtracking/bills081/bills/HB1716.HTM

Healey, J. (2008, January 22). The false promise of Real ID. Los Angeles Times. Retrieved December 20, 2008, from http://www.latimes.com/news/opinion/la-oe-healey22jan22,0,5551102.story?coll=la-opinion-center

Helft, M. (2008, November 11). Google uses searches to track flu's spread. New York Times. Retrieved January 1, 2009, from http://www.nytimes.com/2008/11/12/technology/internet/12flu.html

Hellums, S. (2002). Bits and bytes: The Carnivore initiative and the search and seizure of electronic mail. William & Mary Bill of Rights Journal, 10(April).

Herman, E. S., & Chomsky, N. (1988). Manufacturing consent: The political economy of the mass media. New York: Pantheon.

Heyman, D., & Carafano, J. J., Ph.D. (2008). Homeland Security 3.0: Building a national enterprise to keep America free, safe and prosperous: Center for Strategic & International Studies.

Hoffman, B. (1998). Inside terrorism. London: Victor Gollancz, Ltd.

Hope, C. (2008, October 21). Centuries of British freedoms being 'broken' by security state, says Sir Ken Macdonald. Telegraph. Retrieved February 22, 2009 from http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/3230452/Centuries-of-British-freedoms-being-broken-by-security-state-says-Sir-Ken-Macdonald.html

House Bill No. 1716. (2008, April 8). Missouri 94th General Assembly Retrieved April 24, 2008, from http://www.house.mo.gov/billtracking/bills081/biltxt/perf/HB1716P.htm

Hsu, S. (2007a, October 27). FEMA official apologizes for staged briefing with fake reporters. Washington Post. Retrieved January 12, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2007/10/26/AR2007102602157.html

Hsu, S. (2007b, November 4). Homeland Security Retreats from Facets of 'Real ID'. Washington Post. Retrieved February 24, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2007/11/03/AR2007110300890.html

Hubbard, B. (2008, August 13). Police turn to secret weapon: GPS device. Washington Post. Retrieved January 8, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275.html?hpid=topnews

Hudson, A. (2007, February 14). Chertoff defends Real ID mandate; Change sought in visa waivers. Washington Times. Retrieved February 21, 2009, from http://www.washingtontimes.com/news/2007/feb/13/20070213-111641-9285r/

If you have nothing to hide... (2008, February 14). Chronicles of Dissent. Retrieved January 11, 2009, from http://www.pogowasright.org/blogs/dissent/?p=828

Image of bombers' deadly journey (2005, July 17). BBC News. Retrieved January 1, 2009, from http://news.bbc.co.uk/2/hi/uk_news/politics/4689739.stm#

Intelligence Reform and Terrorism Prevention Act of 2004, 108-458 (2004).

Intelligent Transportation Systems (ITS). (2005, March 18). United we ride. Retrieved January 7, 2009, from http://www.unitedweride.gov/MMS-ITS-3-18-05.doc

Intermec to support first RFID standard for tire tracking and traceability. (Technology Trends). (2002, April 1). Transport Technology Today, from http://www.allbusiness.com/operations/facilities-office-equipment/181020-1.html

Internet and computer monitoring software. (n.d.). Workexaminer Retrieved January 9, 2009, from http://www.workexaminer.com/

Jackson, D. (1999). Protection of privacy in the search and seizure of e-mail: Is the United States doomed to an Orwellian future? Temple Environmental Law & Technology, 17(Spring).

Jenkins, B. (1986). Defense against terrorism. Political Science Quarterly, 101(5), 773-786.

Johnson, C. (1958). The status of freedom of expression under the Smith Act. The Western Political Quarterly, 11(3).

Johnson, C. (2008, October 4). Guidelines expand FBI's surveillance powers. Washington Post. Retrieved February 25, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2008/10/03/AR2008100303501.htm

Johnston, D. (2003, September 9). Two years later: 9/11 tactics; official says Qaeda recruited Saudi Hijackers to strain ties. The New York Times. Retrieved February 25, 2009, from http://query.nytimes.com/gst/fullpage.html?res=9803E4DD14BF93AA3575AC0A9659C8B63

Jonas, J., & Harper, J. (2006). Effective counterterrorism and the limited role of predictive data Mining: Cato Institute. Retrieved February 25, 2009, from http://www.cato.org/pubs/pas/pa584.pdf

Jones, K. C. (2007a, January 22). Thieves busted by GPS-enabled booty Information Week. Retrieved February 25, 2009, from http://www.informationweek.com/story/showArticle.jhtml?articleID=196902643

Jones, K. C. (2007b, August 21). Vermont volunteers for Secure ID. Information Week. Retrieved February 25, 2009, from http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=201801569&cid=RSSfeed_TechWeb

Jones, K. C. (2007, June 1). Web security breach lets cat out of Baghdad embassy plans. Information Week. Retrieved June 5, 2007, from http://www.informationweek.com/shared/printableArticle.jhtml?199900280

Jones, K. C. (2008, March 21). Obama, Clinton, McCain passport breaches expose human, not tech weakness. Information Week. Retrieved December 26, 2008, from http://www.informationweek.com/news/management/showarticle.jhtml?articleid=206905232

Jones, S. (1992). Was there a Hawthorne Effect? The American Journal of Sociology, 98(3), 451-468.

Jordan, L. J. (2007, March 10). Gonzales, Mueller admit FBI broke law. Washington Post. Retrieved October 29, 2007, from http://www.washingtonpost.com/wp-dyn/content/article/2007/03/10/ar2007031000324_pf.html

Jose Padilla. (n. d.). New York Times. Retrieved February 22, 2009, from http://topics.nytimes.com/top/reference/timestopics/people/p/jose_padilla/index.html?inline=nyt-per

Keeping secrets in cyberspace: Establishing Fourth Amendment protection for Internet communication. (1997). Harvard Law Review, 110(May).

Keizer, G. (2007, July 30). Black Hat-bound researcher denied entry into U.S. Computer World. Retrieved January 10, 2009, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9028378&intsrc=news_ts_head

Kerr, J. (2007, April 4). Tire pressure monitoring systems. Canadian Driver. Retrieved January 8, 2009, from http://www.canadiandriver.com/articles/jk/070404.htm

Klein, N. (2008, May 29). China's all-seeing eye. Rolling Stone. Retrieved December 30, 2008, from http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye

Knickmeyer, E. (2008, October 18). Al-Qaeda Web forums abruptly taken offline. Washington Post. Retrieved December 31, 2008, from http://www.washingtonpost.com/wp-dyn/content/article/2008/10/17/AR2008101703367.html

Knopf, A. (1999). Privacy and the Internet: Welcome to the Orwellian world. University of Florida Journal of Law and Public Policy, 11(Fall).

Krebs, B. (2007, July 6). Three worked the web to help terrorists. Washington Post. Retrieved July 10, 2007, from http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945_pf.html

Kronholz, J. (2003, October 28). Reader beware: PATRIOT Act riles an unlikely group: nations librarians; Fears about terrorism clash with principles of privacy as online searches surge; FBI: 'bad guys' use Web, too. The Wall Street Journal (Eastern Edition), p. A. 1. Retrieved February 25, 2009, from ABI/INFORM Global database. (Document ID: 431781101).

Kuhn, M. (2007). Federal dataveillance: Implications for Constitutional privacy protections. New York: LFB Scholarly.

Laqueur, W. (1999). The new terrorism: Fanaticism and the arms of mass destruction. New York: Oxford University Press.

Lawless, M. (2007). The third party doctrine redux: Internet search records and the case for a "Crazy Quilt" of Fourth Amendment protection. UCLA Journal of Law and Technology, 2007(Spring).

Leckrone, S. E. (1997, March 17, 1997). Turning back the clock: The Unfunded Mandates Reform Act of 1995 and its effective repeal of environmental legislation. Retrieved August 3, 2008, from http://law.indiana.edu/ilj/oldsite/volumes/v72/no2/leckrone.html

Lenzer, J. (2006, January 14). Doctors outraged at PATRIOT Act's potential to seize medical records British Medical Journal. Retrieved January 10, 2009, from http://www.bmj.com/cgi/content/extract/332/7533/69

Levey, S. (2006, July 11). Testimony of Stuart Levey, Under Secretary, Terrorism and Financial Intelligence before the House Financial Services Subcommittee on Oversight and Investigations. Retrieved November 23, 2008, from http://www.treas.gov/press/releases/hp05.htm

Levy, R. (2003, August 11). Jose Padilla: No charges and no trial, just jail. Chicago SunTimes Retrieved February 22, 2009, from http://www.cato.org/pub_display.php?pub_id=3208

Lewis, C. (2000). The terror that failed: Aftermath of the bombing in Oklahoma City. Public Administration Review, 60(3), 201-210.

Limbaugh v. Florida (Fourth District Court of Appeal 2004).

Lincecum, G. (2003). Electronic surveillance: Protecting the privacy ecosystem from the Federal Bureau of Investigation's Carnivore. Oklahoma City Law Review, 28 (Spring).

Lipowicz, A. (2007, September 13). Testimony: Clock ticking on Real ID compliance. Washington Technology. Retrieved December 20, 2008, from http://www.washingtontechnology.com/online/1_1/31408-1.html

Liptak, A. (2007, August 13). A case so shielded one side is in the dark New York Times. Retrieved January 10, 2009, from http://select.nytimes.com/2007/08/13/us/13bar.html?_r=1&scp=1&sq=case%20so%20dark%20one%20side%20is%20in%20the%20dark&st=cse

Lofgren, C. (2005, October 11). Hardships of War. Claremont Institute. Retrieved January 11, 2009, from http://www.claremont.org/publications/crb/id.1082/article_detail.asp

Loyalty & Stored Value Cards. (2004). CardLogix. Retrieved January 9, 2009, from http://www.cardlogix.com/pdf/LoyaltyAndStoredValueCards.pdf

MacManus, S. (1991). "Mad" about mandates: The issue of who should pay for what resurfaces in the 1990s. Publius, 21(3), 59-75.

Madigan, N. (2008, July 18). Spying uncovered. Baltimore Sun Retrieved February 20, 2009, from http://www.baltimoresun.com/news/local/bal-te.md.spy18jul18,0,3787307.story

Marek, A. (2007, February 11). Escaping the watch list. U.S. News and World Report. Retrieved January 11, 2009, from http://www.usnews.com/usnews/news/articles/070211/19watch_print.htm

Margolick, D. (1982, June 4). Reprise on McCarran Act: Familiar and forbidding obstacles confront those challenging the latest visa denials. New York Times (1857-Current file),p. B1. Retrieved March 2, 2009, from ProQuest Historical Newspapers The New York Times (1851 - 2005) database. (Document ID: 121563603).

Marx, G. (1974). Thoughts on a neglected category of social movement participant: The agent provocateur and the informant. The American Journal of Sociology, 80(2), 402-442.

McTigue, D. (1999). Marginalizing Individual Privacy on the Internet Boston University Journal of Science and Technology Law, 5(Spring).

McWhirter, D., & Bible, J. (1992). Privacy as a Constitutional Right. New York: Quorum Books.

MD5 weakness allows fake SSL certificates to be created. (2008, December 30). SSL Shopper. Retrieved February 22, 2009, from http://www.sslshopper.com/article-md5-weakness-allows-fake-ssl-certificates-to-be-created.html

METRO Group moves closer to its "Future Store" vision with smart merchandising enabled by RFID. (2008, December 23). IBM. Retrieved January 11, 2009, from http://www01.ibm.com/software/success/cssdb.nsf/cs/jsts-7mlkhs?OpenDocument&Site=software&cty=en_us

Metro opens high-tech shop and Claudia approves. (2003, April 28). IBM. Retrieved January 11, 2009, from http://web.archive.org/web/20040228234802/http://www1.ibm.com/industries/wireless/doc/content/news/pressrelease/872672104.html

Metz, C. (2008). Yahoo! mocks Google privacy theatre. The Register. Retrieved December 23, 2008, from http://www.theregister.co.uk/2008/12/17/yahoo_anonymization_explained/

Milberg, S., Burke, S., Smith, H., & Kallman, E. (1995). Values, personal information, privacy and regulatory approaches. Communications of the ACM, 38(12).

Milcent, G., & Cai, Y. (2006). Object detection and tracking. Ambient Intelligence Lab. Retrieved January 1, 2009, from http://www.cmu.edu/vis/project5.html

Milgram, S. (1967). Small world problem. Psychology Today, 1(1), 61-67.

Milgram, S. (1974). Obedience to authority: An experimental view. New York: Perenial Classics.

Military Commissions Act of 2006. (2006). Washington Post. Retrieved February 22, 2009, from http://www.washingtonpost.com/wpsrv/politics/documents/cheney/military_commissions_act.pdf

Million Dollar Netflix. (2006, October 2). Kiosk.net. Retrieved January 7, 2009, from http://kiosk.net/2006/10/million-dollar-netflix/

Mills, E. (2008, August 6). Hacking electronic-toll systems. CNET News. Retrieved January 7, 2009, from http://news.cnet.com/8301-1009_3-10009353-83.html

Minimum standards for driver's licenses and identification cards acceptable by Federal agencies for official purposes; final rule. (2008). Retrieved from http://edocket.access.gpo.gov/2008/08-140.htm.

Missing persons investigative best practices protocol unidentified deceased persons investigative guidelines. (2008, October 30). New Jersey State Police. Retrieved January 9, 2009, from http://www.njsp.org/divorg/invest/pdf/mpi-best-practices-protocol-103008.pdf

Mousseau, M. (2002/2003). Market civilization and its clash with terror. International Security, 27(3), 5-29.

Murphy, K. (2007, October 19). Britain's long lens of the law. Los Angeles Times. Retrieved February 25, 2009, from http://articles.latimes.com/2007/oct/19/world/fg-bigbrother19

Myers, L., Pasternak, D., & Gardella, R. (2005, December 14). Is the Pentagon spying on Americans? MSNBC. Retrieved February 7, 2009, from http://www.msnbc.msn.com/id/10454316/

Nakashima, E. (2007, December 22). FBI prepares vast database of biometrics. Washington Post. Retrieved October 26, 2008, from http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544_pf.html

Nakashima, E. (2008, January 26). Bush order expands network monitoring. WashingtonPost.com. Retrieved January 7, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=rss_technology

Napolitano, A. (2004, March 5). Repeal the PATRIOT Act. Wall Street Journal. (Eastern Edition), p. A. 14. Retrieved February 25, 2009, from ABI/INFORM Global database. (Document ID: 571244961).

National strategy for combating terrorism. (2006). Washington, D.C.

Newmarker, C. (2007, August 10). E-Z Pass records out cheater in divorce court. MSNBC. Retrieved January 6, 2009, from http://www.msnbc.msn.com/id/20216302/

Nobles, J. (2000). State mandates on local governments. St. Paul, MN: State of Minnesota.

Notice of proposed rulemaking: Minimum standards for driver's licenses and identification cards acceptable by Federal agencies for official purposes. (2007). Retrieved December 1, 2008, from http://edocket.access.gpo.gov/2007/07-1009.htm

O'Harrow, R. (1998, March 8). Are data firms getting too personal. Washington Post. Retrieved November 6, 2008, from http://www.washingtonpost.com/wpsrv/frompost/march98/privacy8.htm

O'Harrow, R. (2005). No place to hide. New York: Simon & Schuster, Inc.

Officer suspended for mailing ‘Homewrecker' flyers. (2008, February 8). WSB-TV. Retrieved January 11, 2009, from http://www.wsbtv.com/news/15256835/detail.html

Official 9/11 death toll climbs by one. (2008, October 4). Retrieved February 25, 2009, from http://www.cbsnews.com/stories/2008/07/10/national/main4250100.shtml

Order pertaining to Al-Haramain Islamic Foundation et al v Bush et al (C 07-0109 VRW). (2009, January 5). United States District Court for the Northern District of California. Retrieved January 10, 2009, from http://www.eff.org/files/filenode/att/alharamainorder10509.pdf

Pabst, G. (2006, March 20). Activist gives her voice to immigrant causes. Milwaukee Journal Sentinel. Retrieved September 28, 2008, from http://www.jsonline.com/story/index.aspx?id=409416

Parent, W. A. (1983). Privacy, morality and the law. In J. Feinberg & H. Gross (Eds.), Philosophy of Law. Belmont, CA: Wadsworth Publishing Company.

Parking ticket management solutions. (2008, August 19). Complus Data Innovations, Inc. Retrieved January 6, 2009, from http://www.complusdata.com/news.asp

Personal identification - AAMVA international specification - DL/ID card design. (2005). American Association of Motor Vehicle Administrators. Retrieved December 27, 2008, from http://www.aamva.org/aamva/documentdisplay.aspx?id={66260ad6-64b9-45e9-a253-b8aa32241be0}

Phillips, D. (2005). Texas 9-1-1: Emergency telecommunications and the genesis of surveillance infrastructure. Telecommunications Policy, 29(11), 843-856.

Phishing explained. (n.d.). APACS - the U.K. payments association. Retrieved January 11, 2009, from http://www.banksafeonline.org.uk/phishing_explained.html

Posner, R. (2006). Not a Suicide Pact. New York: Oxford University Press.

Poulsen, K. (2007, August 15). NSA judge: 'I feel like I'm in Alice in Wonderland.' Wired.com. Retrieved January 10, 2009, from http://blog.wired.com/27bstroke6/2007/08/nsa-hearing-ope.html

Prevent and disrupt terrorist attacks. (2007). White House. Retrieved December 28, 2008, from http://www.whitehouse.gov/infocus/homeland/nshs/2007/sectionv.html

Prince, R. (2008, October 16). Jacqui Smith plans broad new 'Big Brother' surveillance powers. The Telegraph. Retrieved February 20, 2009, from http://www.telegraph.co.uk/news/newstopics/politics/3202766/Jacqui-Smith-plans-broad-new-Big-Brother-surveillance-powers.html

Proposed “enhanced” licenses are costly to security and privacy. (2007, September). EPIC. Retrieved January 11, 2009, from http://epic.org/privacy/surveillance/spotlight/0907/default.html

Pumphrey, G. (2003, June 19). Types of terrorism and 9/11. Retrieved September 28, 2008, from http://www.globalresearch.ca/articles/PUM306A.html

Radil, A. (1999). Document 1: The right to be left alone. The Surveillance Society. Retrieved November 11, 2008, from http://news.minnesota.publicradio.org/features/199911/15_newsroom_privacy/leftalone.html

Ragan, F. (1971). Justice Oliver Wendell Holmes, Jr., Zechariah Chafee Jr., and the clear and present danger test for free speech: The first year, 1919. The Journal of American History, 58(1).

Rao, V. R., & Tripati, R. (2008, November). Personal information integration in e-government. eGov. Retrieved January 9, 2009

Real ID Act of 2005. (2005). Retrieved February 25, 2009, from http://www.ombwatch.org/regs/2005/hr418.pdf

Reilly, R. (1999). Conceptual foundations of privacy: looking backward before stepping forward, Robert A. Reilly. Richmond Journal of Law and Technology, 6(Fall).

Reno, J. (1995). Procedure for contacts between the FBI and the criminal division concerning foreign intelligence and foreign counterintelligence investigations. Washington, D.C.: U.S. Department of Justice.

Report from the field: The USA PATRIOT Act at work. (2004). U.S. Department of Justice.

Report into the London terrorist attacks on 7 July 2005. (2006). Intelligence and Security Committee. Retrieved February 25, 2009, from http://www.official-documents.gov.uk/document/cm67/6785/6785.pdf

Report to the Attorney General and Director of Central Intelligence. (1995).

Reutty, M. (2007). What happened to me when the police came knocking. Computers in Libraries, 27(6), 10-15.

RFID, A vision of the future. (2007). RSA Laboratories. Retrieved January 11, 2009, from http://www.rsa.com/rsalabs/node.asp?id=2117

Risen, J., & Lichtblau, E. (2005, December 15). Bush lets U.S. spy on caller without courts. New York Times. Retrieved January 9, 2009, from http://www.nytimes.com/2005/12/16/politics/16program.html

Rollins, J. (2008). Fusion Centers: Issues and options for Congress: Congressional Research Service - U.S. Congress.

Rotenberg, M. (2006). Real ID, real trouble. Communications of the ACM, 49(3), 128.

Rumsfeld, D. (2001, September 24). DoD news briefing - Secretaries Rumsfeld and Martinez. Retrieved November 17, 2008, from http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=1927

Savage, C. (2008). President weakens espionage oversight. Boston Globe Online. Retrieved December 31, 2008, from http://www.boston.com/news/nation/articles/2008/03/14/president_weakens_espionage_oversight/

Scheck, T. (2006). Hatch wants end to selling of driver's license info. Minnesota Public Radio. Retrieved January 9, 2009, from http://news.minnesota.publicradio.org/features/2006/01/04_scheckt_id/

Schneider, J., & Schneider, P. (2002). The Mafia and al-Qaeda: Violent and secretive organizations in comparative and historical perspective. American Anthropologist, 104(3), 776-782.

Schneier, B. (2006, May 18). The eternal value of privacy. Wired. Retrieved December 10, 2008, from http://www.wired.com/news/columns/1,70886-0.html

Schneier, B. (2007, May 8). Testimony of Bruce Schneier United States Senate Committee on the Judiciary. Retrieved February 20, 2009, from http://judiciary.senate.gov/hearings/testimony.cfm?id=2746&wit_id=6454

Schneier, B. (2007, January 25). In praise of security theater. Wired. Retrieved January 2, 2009, from http://www.wired.com/print/politics/security/commentary/securitymatters/2007/01/72561

Schweitzer, B. (2008, January 18). Letter to Governor Ritter. Wired. Retrieved December 25, 2008, from http://blog.wired.com/27bstroke6/files/real_id_to_gov_ritter_011808_pdf1.pdf

Scowcroft, B. (2002, September 5). Speech: Remarks by Brent Scowcroft at the U.S. Institute of Peace; Conference on America's challenges in a changed world. Retrieved November 17, 2008, from http://www.ffip.com/interviews090502.htm

Severance, C. (2007, November 12). Caught on camera: 300 times a day! Retrieved November 12, 2008, from http://www.winknews.com/news/local/11220536.html

Significant terrorist incidents, 1961-2003: A Brief Chronology. (2004). Retrieved September 27, 2008, from http://www.state.gov/r/pa/ho/pubs/fs/5902.htm

Sim card data recovery software. (n.d.). Datadoctor.org. Retrieved January 8, 2009, from http://www.datadoctor.org/partition-recovery/sim-card.html

Singel, R. (2007, June 12). AT&T “Spy Room” documents released, confirm Wired News' earlier publication. Wired. Retrieved February 22, 2009, from http://blog.wired.com/27bstroke6/2007/06/att_spy_room_do.html

Singel, R. (2008a, January 18). Montana governor foments Real ID rebellion. Wired. Retrieved December 25, 2008, from http://blog.wired.com/27bstroke6/2008/01/montana-governo.html

Singel, R. (2008b, March 21). Montana governor: DHS “blinks” on Real ID. Wired. Retrieved February 25, 2009, from http://blog.wired.com/27bstroke6/2008/03/montana-gov-dhs.html

Skatoff-Gee, M. (1996). Changing technologies and the expectation of privacy: A modern dilemma. Loyola University Chicago Law Journal, 28(Fall).

Slobogin, C. (2007). Privacy at risk: The new government surveillance and the Fourth Amendment. Chicago: The University of Chicago Press.

Smelser, M. (1954). George Washington and the Alien and Sedition Acts. The American Historical Review, 59(2), 322-334.

Smith, R. (2005). Civil liberties in the brave new world of antiterrorism. Radical History Review(93).

Solomon, D. (2006, October 15). For God and country. New York Times Magazine, 22.

Solomon, J. (2007, June 14). FBI finds it frequently overstepped in collecting data. Washington Post. Retrieved June 20, 2007, from http://www.washingtonpost.com/wp-dyn/content/article/2007/06/13/AR2007061302453_pf.html

Solove, D. (2006). A brief history of information privacy law: George Washington University Law School.

Songini, M. (2006, June 12). Wisconsin law bars forced RFID implants. Computerworld. Retrieved February 21, 2009, from http://www.computerworld.com/action/article.do?command=viewarticlebasic&articleid=111542

Songini, M. (2007, April 12). N.D. bans forced RFID chipping. Computerworld. Retrieved February 21, 2009, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9016385

Spafford, E. (2006, December 18). Quotable Spaf. Gene Spafford's personal pages. Retrieved January 2, 2009, from http://homes.cerias.purdue.edu/~spaf/quotes.html

Spafford, E. (2008, September 3). Security through obscurity. CERIAS. Retrieved February 21, 2009, from http://www.cerias.purdue.edu/site/blog/post/security_through_obscurity/

Spinetto, N. (2008, February 7). Deputy fired. WINK-TV News. Retrieved January 11, 2009, from http://www.winknews.com/news/local/15408931.html

Spy my ride: Somebody may be tracking your vehicle and you don't know about it! (n.d.). HexVeiw. Retrieved January 8, 2009, from http://www.hexview.com/sdp/node/44

Standards - U.S. License Technology. (2008). American Association of Motor Vehicle Administrators. Retrieved December 27, 2008, from http://aaa.aamva.org/knowledgecenter/standards/uslicensetechnology.htm

Statement on HR 199. (2006, March 9, 2006). Office of the Secretary. Retrieved November 20, 2007, from http://www.whitehouse.gov/news/releases/2006/03/20060309-8.html

States Challenge Homeland Security's ID Deadline. (2008). ATIPShop. Retrieved fromhttp://atipshop.com/index.php?option=com_content&task=view&id=21&Itemid=1

Stobart, J., & Rotella, S. (2008, August 2). Jury fails to reach verdict in London attacks. Seattle Times. Retrieved January 1, 2009, from http://seattletimes.nwsource.com/html/nationworld/2008087486_london02.html

Stone, G. (2003). Civil liberties in wartime. Journal of Supreme Court History, 28(3).

Strickland, L. S., & Hunt, L. E. (2005). Technology, security, and individual privacy: New tools,new threats, and new public perceptions. Journal of the American Society for Information Science and Technology, 56(3).

Strub, H. (1989). The theory of panoptical control: Bentham's panopticon and Orwell's Nineteen Eighty Four. The Journal of Behavioral Sciences, 25, 40-59.

Sullivan, B. (2006, October 19). 'La difference' is stark in EU, U.S. privacy laws. MSNBC. Retrieved January 10, 2009, from http://www.msnbc.msn.com/id/15221111/

Svensson, P. (2008, March 24). HD videoconferencing: In your living room. USA Today. Retrieved January 3, 2009, from http://www.usatoday.com/tech/products/2008-03-24-hd-videoconferencing-home_N.htm

SWIFT to stop processing EU banking data in the US. (2007, October 15). The Register. Retrieved October 17, 2007, from http://www.theregister.co.uk/2007/10/15/swift_processing_halt/print.html

Tankersley, J. (2007, November 16). Audit: Terrorists got U.S. aid: Agency's screening called inadequate. Chicago Tribune. Retrieved January 11, 2009, from http://archives.chicagotribune.com/2007/nov/16/news/chi-terror_aid16nov16

Temple-Rastin, D. (2007a, September 9). Enemy within? Not quite. Washington Post. Retrieved January 11, 2009, from http://www.washingtonpost.com/wp-Dyn/content/article/2007/09/07/AR2007090702049.html

Temple-Rastin, D. (2007b, July 4). In U.S., calls grow for U.K.-style security cameras. All Things Considered, NPR. Retrieved January 1, 2009, from http://www.npr.org/templates/story/story.php?storyId=11737314

Terrorism, Al Qaeda, and the Muslim world. (2003, July 9). Hearing of the National Commission on Terrorist Attacks Upon the United States, Washington, D.C.

Thompson, S. (1999). The digital explosion comes with a cost: The loss of privacy. Journal of Technology Law & Policy, 4(Spring).

Tilly, C. (2004). Terror, terrorism, terrorists. Sociological Theory, 22(1), 5-13.

Top Al Qaeda leader Abu Ubaida al-Masri confirmed dead in Pakistan. (2008, April 9). Fox News. Retrieved January 1, 2009, from http://www.foxnews.com/story/0,2933,348668,00.html

Tortora, V. R. (1998). The seventh sense. Focus, 45(1), 15-18.

Tushnet, M. (Ed.). (2008). I Dissent. Boston: Beacon Press.

Twelve Senators urge Frist to keep Real ID Act off Supplemental Appropriations Bill: Sweeping proposal needs deliberate consideration. (2005, April 11). Retrieved December 20, 2008, from http://hsgac.senate.gov/public/index.cfm?FuseAction=PressReleases.Print&PressRelease_id=b456811f-b97a4d4c8503cacbaaa649ca&suppresslayouts=true

U.S. automobile registrations. (2001). Retrieved 2008, October 25, from http://vnweb.hwwilsonweb.com/hww/results/results_single_fulltext.jhtml?_DARGS=/hww/results/results_single.jhtml.14

Understanding the realities of REAL ID: A review of efforts to secure drivers licenses and identification cards, U. S. Senate (2007).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) ACT of 2001. (2001).

Vanderhoof, R. (2007). Executive director's letter. Smart card talk. Retrieved December 27, 2008, from http://www.smartcardalliance.org/newsletter/march_2007/letter_0307.html

Vermont Issues New Enhanced Driver's License. (2009, January 5). AAMVA. Retrieved January 11, 2009, from http://www.aamva.org/Publications/TWiR/2009/Month01/Day05/VTEDLID.htm

Vijayan, J. (2008, December 8). GPS tracking of high credit-risk drivers: Good practice or privacy violation? ComputerWorld. Retrieved January 8, 2009, from http://blogs.computerworld.com/gps_tracking_privacy_violation

Vlahos, J. (2008, January). Surveillance society: New high-tech cameras are watching you.Popular Mechanics. Retrieved January 6, 2009, from http://www.popularmechanics.com/technology/military_law/4236865.html?page=2

Volokh, A. (1997). n guilty men. University of Pennsylvania Law Review 146.

Warren, S., & Brandeis, L. (1890). The right to privacy. Harvard Law Review, 4(5).

Warrior, J., McHenry, E., & McGee, K. (2003). They know where you are. IEEE Spectrum, 40(7), 20-25.

Warshak v. United States: Federal appeals court holds email constitutionally protected. (2007, July 24). Center for Democracy and Technology. Retrieved February 5, 2009, from http://www.cdt.org/security/20070726warshak-analysis.pdf

Washburn, G. (2007, August 12). City rakes in revenue from tickets: Car-related fines plug $210 million hole in budget. Chicago Tribune. Retrieved January 6, 2009, from http://archives.chicagotribune.com/2007/aug/12/news/chi-carcash_bd_12aug12

Welch, M. (2003). Get Ready for PATRIOT II. Journal. Retrieved from http://www.alternet.org/module/printversion/15541

Will Real ID actually make us safer? An examination of privacy and civil liberties concerns, United States Senate, 110th Congress, First Sess. 1-247 (2007).

Williams, I. (2007). US state bans forced RFID tagging of humans. VNUNet.Retrieved from http://www.vnunet.com/articles/print/2197977

Wolf, N. (2007). The end of America. White River Junction, VT: Chelsea Green Publishing Company.

Yoo, D. (1996). Review: Captivating memories: Museology, concentration camps, and Japanese American history. 48(4), 680-699.

Yoo, J. (2006). War by other means. New York: Atlantic Monthly Press.

Young, P. (2001). The case against Carnivore: Preventing law enforcement from devouring privacy. Indiana Law Review, 35.

Zalud, B. (2007, April). Real ID or no Real ID? Security, 51.

VITA

# VITA

William Eyre
U.S. Senate – Sergeant at Arms
Technology Development Services
Washington, D.C. 20510
202-224-8583

Publications and Presentations:

(2007). *Comparative Effectiveness of Least Significant Bit Steganography Containing Varying Amounts of Encrypted and Unencrypted Content in Evading Detection By Blind Steganalysis.* Purdue University, West Lafayette. (thesis)

(2007). *Emerging Trends in Digital Forensics.* West Lafayette. (presentation)

(2007). *Biometrics and Privacy*. West Lafayette: CERIAS – Purdue University. (poster)

(2006). *Steganography and Terrorist Communications: Current Information and Trends – Tools, Analysis and Future Directions in Steganalysis in Context with Terrorists and Other Criminals.* Paper presented at the Conference on Digital Forensics, Security and Law, Las Vegas, NV.

*Education:*

Purdue University – CERIAS W. Lafayette, IN 2009
Ph.D. Student – Information Security
Information security management, public policy, information security policy, project management, telecom management and homeland security.

Purdue University – CERIAS W. Lafayette, IN 2007
MS Information Security
Biometrics, cryptography, digital forensics, cell phone forensics, computer & network security, international terrorism, and statistics.

Northeastern Illinois University Chicago, IL 2005
BS – Computer Science. Cum Laude.

Northwestern University Evanston, IL 1978-1983
Pursued a BS in Computer Science.

Massachusetts Institute of Technology Cambridge, MA 1977-1978
Core engineering courses.

Culver Military Academy Culver, IN 1974-1977
Completed the four-year course of study in three years. National Merit Scholar.

Experience:
United States Senate Washington, DC 5/2008 - present
Senior Information Security Services Specialist
Incident response lead. Lead virtualization and VoIP projects.

Secure Anchor Consulting LLC Herndon, VA Summer 2006
Project Manager/Lead Consultant
Developed VoIP network security training course. Communication liason duties.

Superior Information Systems Chicago, IL 1995-2005
Project Manager/Lead Consultant
Designed and implemented IT projects. Responsible for client development, proposal generation and system implementation. Mapped responsibilities of staff and supervised my contractors and clients' IT staff in implementing a diverse range of networks, systems and configurations.

Pro Sport Software Chicago, IL 1983-1995
Designed, developed, coded and tested applications in 3GLs including TurboPASCAL and C/C++ for PC and Mac platforms.
Projects included:
Application suite for management of forensic (speech and debate) tournaments for educational market.
Sports statistical and team management programs.
Management packages for various recreational activities (consumer).