2006

Public Policy and Technology: Advancing Civilization at the Expense of Individual Privacy

Aaron D. Sanders

Public Policy and Technology: Advancing Civilization at the Expense of Individual Privacy

By

Aaron D. Sanders

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

May 2006

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in Information Technology

Thesis Approval Form

Student Name: Aaron Sanders

Thesis Title: Public Policy and Technology: Advancing Civilization at the Expense of Individual Privacy

Thesis Committee

Name	Signature	Date

Prof. William Stackpole
Chair

Charles Border, Ph.D.
Committee Member

Prof. Ronil Hira
Committee Member

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College

of

Computing and Information Sciences

Master of Science in Information Technology

Public Policy and Technology: Advancing Civilization at the Expense of Individual Privacy

I, Aaron Sanders, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: _____ Signature of Author: Aaron Sanders

Abstract

Technological advances have created a new existence, providing an unforeseen level of interaction and transaction between parties that have never physically met. Preliminary thinking was that these advances would create a previously unimaginable level of privacy and anonymity. While a surface examination suggests an abundance of privacy in modern society, a more thorough examination reveals different results. Advances in technology and changes in public policy have produced a world in which a startling amount of information is available regarding a given individual. Rather than experiencing an increase in individual privacy, modern societies suffer from rapidly decreasing individual privacy.

Table of Contents

Introduction

Cultural Influences

Before examining the current situation, it is insightful to examine the opinions of popular culture. Fritz Lang's "Metropolis" (1927) was one of the first movies to explore the possibility of humanity's dark future. Ayn Rand's "Anthem" (1946) focused on philosophical struggles in a future where individuals did not choose their profession or spouse, and individuals identified each other by a number rather than name. Although a vehicle for spreading objectivism, "Anthem" did suggest the notion that a unique number could mean more than an individual's name, as the SSN (Social Security Number) often does in modern society. Next was George Orwell's landmark "1984", which introduced familiar phrases such as "Thought Police" and "Big Brother". "1984" presents a future where the government monitors individuals 24 hours a day, and even their own thoughts are not private. The novel coined the phrase "Big Brother is watching". "The 'Net" (1995) introduced a world in which all of an individual's personal information was available in digital form and stored in massive databases. The film highlighted the fact that one mistaken entry could ruin an individual's life. In the movie, a criminal cracker alters all of the warehoused information regarding the main character, causing law enforcement to identify her as a criminal. "Minority Report" (2002), introduced a future in which police can prevent crimes before they happen by predicting the future. In addition, the film presents a future where biometric technology is ubiquitous. At one point, the main character is walking down a street, and biometrics-enabled billboards scan his retina and change their advertising to suit his preferences.

Definition of Privacy and Privacy Measurement

Although it may seem to possess a proper definition, the word "privacy" requires clarity. The problem is that what privacy *has been* and what privacy *is* do not guarantee what privacy *will be* or what privacy *could be*. For that reason, the best definition of privacy is "control". When this thesis discusses an individual's right to privacy, it is referring to their right to have control over their personal information. Privacy does not mean secrecy, as an individual may freely share their personal information with everyone, if they so desire. Individual privacy focuses on an individual's right to have *control* over their information, allowing the sharing of their personal information only with their explicit permission.

Privacy is critical because it enables individuals to feel safe, secure and in control of their lives. A feeling of privacy allows individuals to set limits that make them feel protected from the outside world. In addition, privacy can influence an individual's behavior, particularly in their shopping behaviors. Studies have found that an individual's shopping behavior can vary greatly given their feelings of trust towards an organization and their desired level of privacy protection (Glen Nowak, Joseph Phelps, and Giles D'Souza "Antecedents and"; Sheena Mitchell "The new").

Measuring privacy is difficult, as there is little prior knowledge on the subject of privacy measurement. In addition, measuring privacy attempts to put quantitative values on qualitative personal feelings, which each individual might perceive differently. This thesis measures privacy as the "level of privacy as it *should* effect *all* individuals". This thesis defines a "Privacy Level Indicator" with a scale of 1 through 5, with 1 being the least invasive and 5 being the most invasive. The defined levels are: **1-Controlled**, **2-Acceptable**, **3-Uncomfortable**, **4-Threatened**, **5-Uncontrolled**. To add finer granularity, the scale contains quarter points. This

provides the ability to show a much more specific analysis of an event's effect on the "level of privacy" during the point in time when the event occurred.

One similar measurement of the level of privacy is that of EPIC's (Electronic Privacy Information Center) Privacy Threat Index. EPIC designed the index after September 11, 2001 to mirror the DHS' (Department of Homeland Security) Terrorism Threat Index. The Privacy Threat Index contains 5 levels, each identified by a color and descriptive label. This thesis does not utilize EPIC's Privacy Threat Index for two reasons. First, it was desirable to use quarter points between each integer level, to provide a finer analysis of each threat. In addition, this thesis looks to apply its designed scale to specific points in history, to determine the extent to which privacy has changed over time, ending with a current level of privacy. Those two objectives could not be met using EPIC's scale, although their scale is an important factor in determining the level of privacy for recent events.

Most of the existing research has focused on the importance of privacy in specific situations, the value of privacy, or methods of benchmarking the effectiveness of privacy preservation methods. The AMA (American Medical Association) has created the Ethical Force Program, to develop performance measures for ethics in healthcare. Novak, Phelps, and Elizabeth Ferrell (2000) studied whether consumers' privacy concerns affected their willingness to provide their personal information during transactions. Nowak, Phelps, and D' Souza (2001) created an empirical study of how privacy concerns effect consumers. Christina Cary, Pruthikrai Mahatanankoon, and H. Joseph Wen (2003) studied methods of preserving individual privacy during the SDLC (Systems Development Lifecycle) and during data mining. Many researchers have studied methods of preserving privacy in data mining.[1] Numerous researchers have studied

[1] For a comprehensive list, visit http://www.cs.umbc.edu/~kunliu1/research/privacy_review.html.

how privacy concerns affect the behavior of online consumers. Although many researchers have studied the ways that privacy affects consumers and organizations, little research exists regarding the effects of outside events on the availability of privacy. This thesis seeks to focus on that area and address the following hypothesis:

H1: Changes in public policy and technological advances have greatly reduced the level of individual privacy in modern society.

Panoptic Sort and Persistent Digital Nym

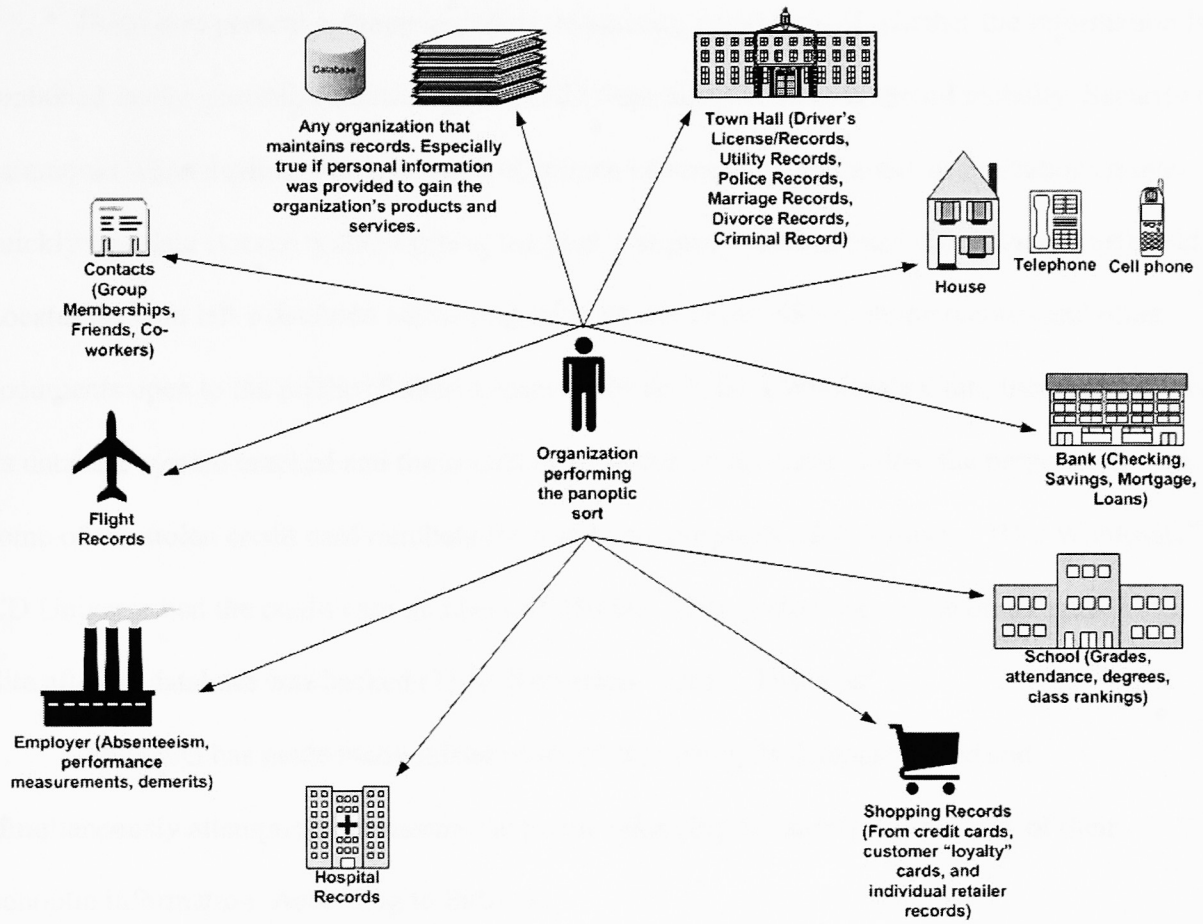
The goal of proving that modern society is actually less anonymous and less private requires the definition of a number of terms. The first term is the panoptic ("all seeing") sort. In "The Panoptic Sort: A Political Economy of Personal Information" Oscar Gandy provides the following definition of a panoptic sort:

> "The panoptic sort is the name I have assigned to the complex technology that involves the collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy. The panoptic sort is a system of disciplinary surveillance that is widespread, but continues to expand its reach" (qtd. in Alex Wexelblat 101).

As described, the design of a panoptic sort is to collect, store, and mine data describing all possible aspects of an individual's existence, including personal, public, educational, professional, political, legal, financial and recreational. In a panoptic sort, the entity performing the sort operation retrieves information from any organization that possesses information describing the individual in question. Organizations possessing information could include libraries, credit card companies, credit bureaus, supermarkets, retail stores, IRS (Internal

Revenue Service) records, DOT (Department of Transportation) records, movie rental records, criminal records, medical records and any other organization possessing records pertaining to the individual in question. The potential uses for the information gained from a panoptic sort are virtually unlimited, and depend on the needs of the organization performing the sort. Potential investigating organizations include world governments, marketing agencies, credit card companies and retail firms. In the US (United States), the government is the largest purchaser of personal information.

This thesis presents a new term for "personal information" with a more concrete definition: panoptic information. Panoptic information is defined as "All of the attributes that describe an individual personally, physically, medically, educationally, politically, legally, financially, mentally, emotionally, locationally and professionally". In more common language terms, panoptic information is any piece of information that describes any attribute that relates directly or indirectly to a given individual. This thesis seeks to examine the many ways that an organization may gather pieces of an individual's panoptic information. Organizations can perform minimal information gathering through the panoptic sort, in which an entity wishing to gather information regarding an individual does so by contacting all of the various other organizations that possess the information. A more intensive information gathering process involves an organization creating and maintaining its own database of an individual's panoptic information, such as the one under development by the USG (United States Government). This centralized data store allows an entity to obtain an individual's panoptic information without having to contact other organizations to retrieve the information, especially when using the information multiple times. The following diagram describes the operation of a panoptic sort:



The modern panoptic sort, whether conducted by a corporate or government entity, follows the three-step process identified by Wexelblat: identification, classification, and assessment (104). First, an organization desires to identify every individual residing within a country's borders. Next, the organization classifies and categorizes residents identified in the first step into groups. For example, a current procedure might classify individuals on the likelihood that they are a terrorist. Finally, the organization would statistically assess each individual against their group as a whole to determine variance and attempt to predict future outcomes.

Databases present a dangerous threat to privacy, regardless of whether the information is contained in one centralized database, or culled from many databases spread globally. Security is paramount when dealing with any piece of private information, and many organizations move quickly into data storage without taking the proper security precautions: A developer mistake at LocatePlus.com left a database containing millions of names, SSNs, phone records and other documents open to the public (Robert Lemos "Slip-up"). BJ's Wholesale Club, Incorporated saw its database system cracked and thousands of customer credit cards stolen; the perpetrator used some of the stolen credit card numbers for fraudulent purposes (Bob Sullivan "BJ's Wholesale"). CD Universe had the credit card numbers of 350,000 of its customers posted on a rogue Web Site after its database was hacked (Troy Wolverton "AmEx, Discover").

The USG has made many mistakes while increasing its database usage and simultaneously attempting to reassure the public regarding the safety and privacy of their panoptic information. According to Sullivan,

"A government subcontractor posted the names, birthdays and daily whereabouts of hundreds of upstate New York children to the Internet, where the information remained publicly available for weeks until MSNBC.com notified authorities...The computer data -- which also listed the names, addresses and other details of low-income and foster families -- passed through three layers of subcontractors on its journey to the Internet ("Government agency").

The USG exercises minimal control and oversight when handling panoptic information, yet it expects this country's residents to feel confident in the USG's ability to manage its citizens' data. According to Sullivan, "The information revealed was explicit. In addition to names, birthdays, and other personal information, a memo field in the database chronicled each child's daily routine..." ("Government agency"). Organizations desiring to possess personal information

regarding a given individual must focus on data security, or risk exposing that individual's life history to the global community. The threat from centralized databases and panoptic sorts combined with the threat from human error and crackers requires an increase in the Privacy Level Indicator of ¼, to 1.25. Although the combination of panoptic sorts and vast data warehouses creates an enormous potential for information misuse, we have not yet knowingly experienced such a data retrieval and storage operation on a grand scale. An increase in the Privacy Level Indicator greater than ¼ point cannot be justified, as no organization has demonstrated the capability of executing a large-scale panoptic sort.

Two related terms requiring definition are "true name" and "persistent digital nym". Vernor Vinge coined the term "true name" in his essay "True Names", written in 1981. True name is the term given to an individual's legal name in the physical world. People use their true name in signing checks, using their driver's license, in conversation and through other common daily activities. The opposite of a true name is a persistent digital [pseudo]nym, which is the name that an individual uses in the electronic ("virtual") world (Timothy C. May 44). Although some individuals may use their true name in the virtual world, most people create a persistent digital nym. The persistence of the digital nym is crucial to the success of the panoptic sort or a centralized database. In the digital world, individuals may pretend to be anyone or anything they desire. Individuals often create a persona to represent themselves in the digital world, and use that persona for everything they do, usually selecting the same username for every site registration, instant messenger (IM) username, eMail address, newsgroup posting or other communication. This behavior adds persistence to the digital nym, so that its path through the virtual world is easily traceable and distinguishable. In addition, the persistent digital nym may develop its own separate personality and existence from that of the true name it represents.

According to May, "...behaviors can and will be attributed to nyms. Some nyms will establish the reputation of being straight in dealings, others will establish a less savory reputation" (66). The persistent digital nym makes following a person through the virtual world easier, rendering the virtual world anything but anonymous. This thesis will present a case study to support this claim.

In some ways, the origination of persistent nyms and true names dates back to colonial times, when many people were illiterate. An illiterate individual would "make their mark" to sign a document, which involved placing an "x" or a "personalized" scribble on the signature line. By using the same mark on every document, a person was able to establish a persona and signature for themselves, even though they could not read or spell their true name. In modern society, persistent nyms have existed in urban landscapes for years. Graffiti artists often paint the same symbol on every object they vandalize. This symbol, known as a "tag" (the process of spraying graffiti on an object is called "tagging"), represents the person that painted the graffiti, and is a signature that they were once in that location.

Liberty and Passport: Persistent Digital Nyms go Corporate

The corporate term for persistent digital nym is digital identity. Digital identities are a growing trend in IT (Information Technology).[2] According to David Greenfield, "At the highest level, a digital identity represents an individual's identity online. This identity consists of a username and attributes of that individual, such as a password, or even personal information..." (41).

The two platforms for persistent digital nyms are Microsoft's Passport and the Liberty Alliance's Project Liberty (Greenfield 40). The purpose of the two competing persistent digital

[2] This paper chooses to use the term persistent digital nym, because it emphasizes the sense of longevity and permanence, which better suits this paper's intended purpose.

nym platforms is to create a SSO (Single Sign-On) environment and personal information store for individuals and organizations. The corporate world has been the first to adopt the idea of persistent digital nyms as a cost saving effort (Greenfield 40). The benefit of SSO to organizations is that it simplifies the authentication process for end users that require access to multiple domains and enables automatic sign-on to applications that are SSO aware.

The efforts put forth by Microsoft and the Liberty Alliance give consumers and employees good reason to adopt a persistent digital nym, and potentially associate it with information from the physical world. When an individual signs up with Passport (http://www.passport.com), they must provide a large amount of personal information, including first and last name, country, state, zip code, time zone, gender, birth date and occupation. Passport does present an individual with choices regarding how much of the information they desire to share with other companies. Microsoft initially aimed Passport at the typical end-user browsing and shopping on the Web, and the service is making inroads in that market. One of the keys to the success of the Passport system is its adoption by "member sites" that support Passport's features. For example, eBay now allows a user to sign on to the auction site using their Microsoft Passport, rather than setting up a new account for use only with eBay. This allows an individual to create one account (using Passport) and then use it on any site that accepts Passport logins. This mirrors operations in the physical world: One does not have a separate driver's license for every store at which they might want to shop and write a check. Instead, they have one driver's license that every store accepts as valid ID (Identification). Gaining widespread adoption of Passport might pose a problem, as the Passport system is a Microsoft controlled system, with no other large industry partners standing behind it.

Currently, Liberty is in the development stages, and appears to be more oriented towards the corporate customer. As such, consumers cannot receive an ID from Liberty. Liberty has a much more open policy, and the support of many influential technological companies. It appears that Liberty is poised and ready to dominate the corporate market.

If Passport or Liberty spur the adoption of persistent digital nyms in the corporate environment, biometrics and the digitalization of one's physical characteristics may be added to their persistent digital nym, and consequently, to data stores. Organizations are increasing their adoption of biometric measures such as fingerprint or retina scanning for the identification and authentication of a given individual. The increased use of biometrics means that an individual's fingerprints or retinal scan would be stored with the organization's chosen identity provider. One problem with biometrics is that coordinated attacks threaten all forms of digitized information. According to Simson Garfinkel, "...fingerprints do not really identify a person: they merely link a particular finger to a record in a file. Change the file, and you change the identification" (44). Garfinkel continues, "Once a biometric is stored inside a computer, all of the security provided by the biometric identification is lost. A stored biometric could easily have been copied from another computer, rather than being discreetly measured" (65). Security is paramount if digital information stores are going to be successful, and security experts have cracked Microsoft's Passport system multiple times[3] (Greenfield 43). In the final months of 2004, many organizations withdrew support for the Passport service, and stopped using it for their identity management needs. The most notable was eBay, who discontinued their support for Passport-based authentication.

[3] For more on the weaknesses of Microsoft's Passport, see Marc Slemko's papers at http://alive.znep.com/~marcs/passport.

Although one of the effects of these technologies was to increase privacy by providing individuals with a method of positively identifying themselves, persistent digital nyms had a greater effect on reducing privacy. Persistent digital nyms greatly enable the aggregation of an individual's panoptic information, because they provide a consistent name for organizations to use in their queries. An organization that supports Passport or Liberty could use its list of registered members' persistent digital nyms and passwords to retrieve their banking, travel, and other panoptic information from other organizations that support Passport or Liberty. In addition, these platforms require perfect security implementation, or risk opening their massive networks and individuals' panoptic information to the cracker community. For these reasons, persistent digital nyms increase the Privacy Level Indicator to 1.75. The ½-point increase in the Privacy Level Indicator is twice the ¼-point increase attributed to panoptic sorts and data warehouses, signaling that persistent digital nyms pose twice the treat to individual privacy. The case study will fully justify the increase attributed to persistent digital nyms by demonstrating a sample of the volume of information that persistent digital nyms can provide.

Computer Technology

The following section provides a sampling of design and implementation flaws that put users' privacy and security at risk. The threats are increasing daily at a rate that makes it nearly impossible to monitor every issue and flaw. The issues examined in the following section provide examples from all of the major areas relating to computing technology.

Protocol Flaws

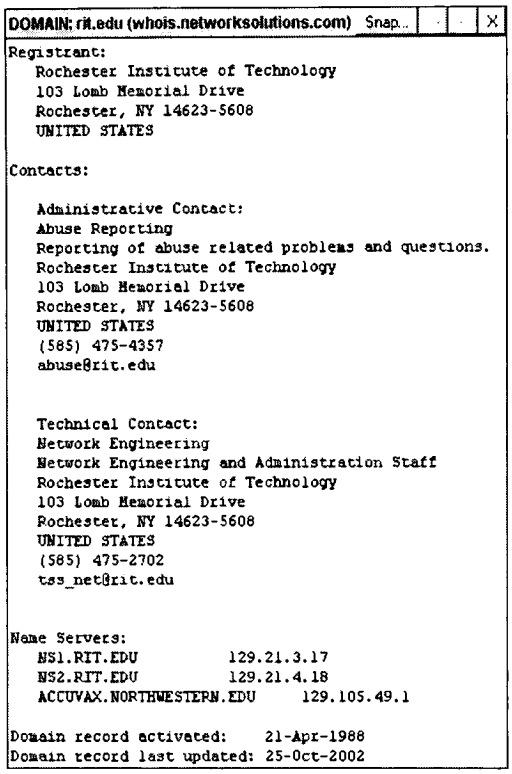
Most of the networking protocols and tools in use today originated decades ago in the late 1960s, before the conception of ubiquitous computing. The rapid rate of technological advancement in the last decade has lead to the discovery of performance and security problems

in many of the protocols that comprise the TCP/IP (Transmission Control Protocol/Internet Protocol) suite. These are critical flaws, as the protocols of the TCP/IP suite comprise the fundamental operations of the Web and Internet.

One problematic tool is the WHOIS command. As its name suggests, WHOIS retrieves information regarding a given individual's identity, specifically the identity of a domain's registrant. When an individual or organization registers a domain name, they are required to provide contact information for the individual charged with administering the registered domain. The problem is that much of this information is unnecessary as contact information, and presents a serious violation of the registrant's privacy.

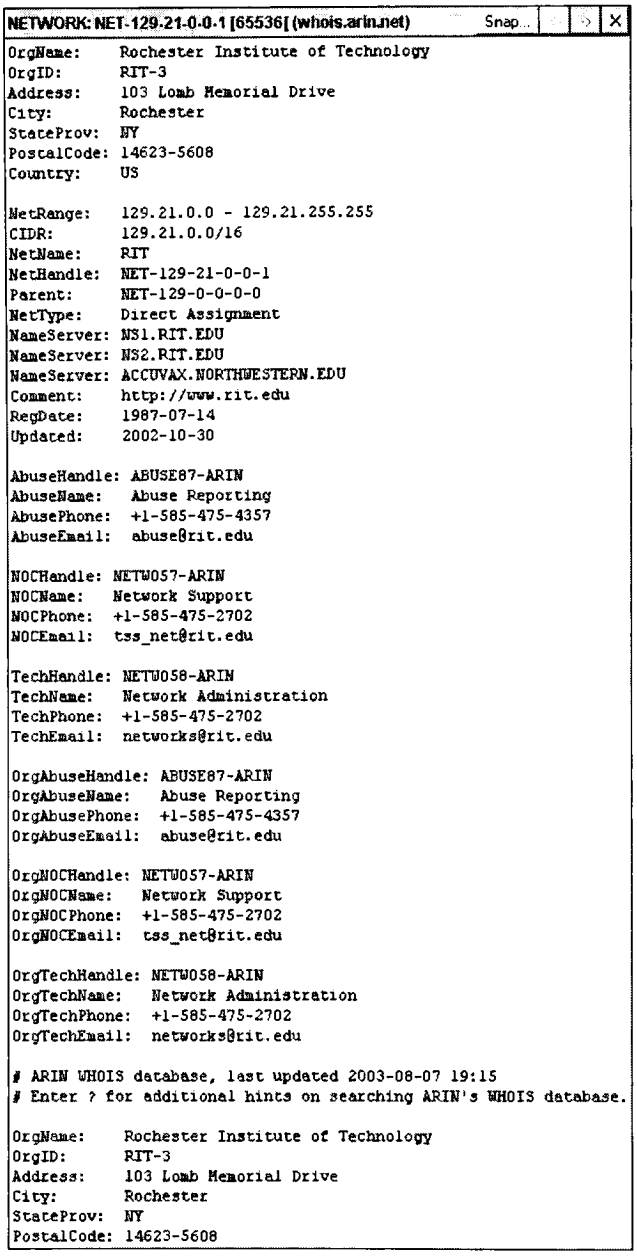
Many shareware, freeware and commercial programs are available for executing a WHOIS lookup on a domain name. One of the best programs available is VisualRoute, which combines many essential networking tools into one package. According to Aaron D. Sanders: "VisualRoute is a **ping**, **whois**, and **tracert** program that displays the results of its tests in a table and on a world map. VisualRoute can trace the route to an IP address or domain name, and return the IP address, node name (including registrant, administrative contact, address, phone number, when the domain lease ends, and IP addresses of the domain's DNS servers), worldwide geographic location (including latitude and longitude), time zone, elapsed response time in milliseconds, and network provider (including IP address block, DNS server IP addresses, mailing address, and telephone number). VisualRoute returns this information for every hop along the way, only failing at the end, if the destination network is set to block the Internet Control Message Protocol (ICMP) packets used by the **ping** command" (7).

VisualRoute gathers most of the displayed information from a WHOIS lookup to the queried domain name. The following figure shows the WHOIS information retrieved using VisualRoute 7.0g to analyze http://www.rit.edu:



As shown in the screen capture, the information returned by the WHOIS query can be extremely personal. The risk is minimal for organizations that register domain names, since most of the information is public contact information for the organization. For an individual that registers a domain name, the information could be very personal, including their home address and telephone number.

One piece of dangerous information for business registrants is the fully qualified domain names and IP addresses for the DNS (Domain Name System) servers that serve the domain. A WHOIS reply also contains information about the network housing the domain. The following figure shows the network provider information for the query to http://www.rit.edu:



```
NETWORK: NET-129-21-0-0-1 [65536] (whois.arin.net)                Snap...
OrgName:     Rochester Institute of Technology
OrgID:       RIT-3
Address:     103 Lomb Memorial Drive
City:        Rochester
StateProv:   NY
PostalCode:  14623-5608
Country:     US

NetRange:    129.21.0.0 - 129.21.255.255
CIDR:        129.21.0.0/16
NetName:     RIT
NetHandle:   NET-129-21-0-0-1
Parent:      NET-129-0-0-0-0
NetType:     Direct Assignment
NameServer:  NS1.RIT.EDU
NameServer:  NS2.RIT.EDU
NameServer:  ACCUVAX.NORTHWESTERN.EDU
Comment:     http://www.rit.edu
RegDate:     1987-07-14
Updated:     2002-10-30

AbuseHandle: ABUSE87-ARIN
AbuseName:    Abuse Reporting
AbusePhone:  +1-585-475-4357
AbuseEmail:   abuse@rit.edu

NOCHandle:  NETW057-ARIN
NOCName:    Network Support
NOCPhone:   +1-585-475-2702
NOCEmail:   tss_net@rit.edu

TechHandle:  NETW058-ARIN
TechName:    Network Administration
TechPhone:   +1-585-475-2702
TechEmail:   networks@rit.edu

OrgAbuseHandle:  ABUSE87-ARIN
OrgAbuseName:    Abuse Reporting
OrgAbusePhone:   +1-585-475-4357
OrgAbuseEmail:   abuse@rit.edu

OrgNOCHandle:  NETW057-ARIN
OrgNOCName:    Network Support
OrgNOCPhone:   +1-585-475-2702
OrgNOCEmail:   tss_net@rit.edu

OrgTechHandle:  NETW058-ARIN
OrgTechName:    Network Administration
OrgTechPhone:   +1-585-475-2702
OrgTechEmail:   networks@rit.edu

# ARIN WHOIS database, last updated 2003-08-07 19:15
# Enter ? for additional hints on searching ARIN's WHOIS database.

OrgName:     Rochester Institute of Technology
OrgID:       RIT-3
Address:     103 Lomb Memorial Drive
City:        Rochester
StateProv:   NY
PostalCode:  14623-5608
```

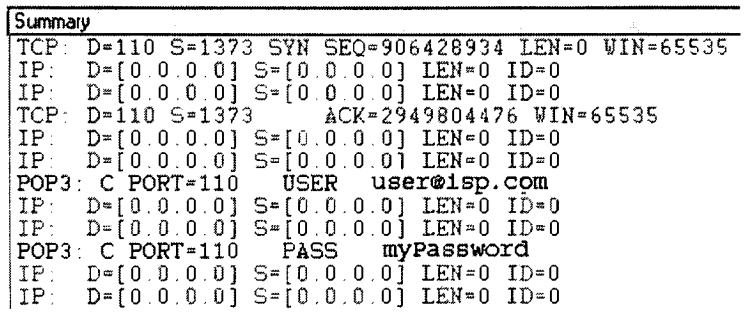
Again, most of the information contained in this response is not that damaging to the organization. One exception is the information contained in the second section, specifically the NetRange and CIDR (Classless Inter-Domain Routing) lines. The NetRange value specifies the block of IP addresses allocated to RIT (Rochester Institute of Technology). This gives an attacker a sense of the size of the network (and often the organization) in question, as well as listing the specific numerical range assigned to that organization. Providing the network range

and server address information in the WHOIS database provides crackers, spammers and other undesirables with information to enhance their attacks.

The questions regarding the information contained in the WHOIS database has caused ICANN (Internet Corporation for Assigned Names and Numbers) to consider a policy redefining the information required during the domain registration process. One of the driving forces behind the WHOIS consideration is EPIC (Electronic Privacy Information Center - http://www.epic.org/privacy/whois/). Unfortunately, ICANN has never had the best interests of the Internet or users in mind, and developing an official policy on WHOIS has dragged on for over four years. In the meantime, some registrants have decided to resolve matters on their own. NameSecure, a domain registrant since 1995, allows its customers to sign up for a service that will mask their personal data in the WHOIS database. When an individual performs a WHOIS query for a domain that uses NameSecure's WHOIS privacy service, the contact information returned will be for NameSecure, not the organization responsible for the domain. NameSecure will then forward any legitimate correspondence to the appropriate recipient.

Another problem related to the TCP protocol suite is that of eMail delivery, especially in the case of the POP3 (Post Office Protocol version 3) and IMAPv4 (Internet Message Access Protocol version 4) protocols. These protocols handle user authentication and storage of eMail messages on the server. The problem with these two protocols is that by default they do not encrypt the connection between the client and the server. For this reason, eMail usernames, passwords and message content are available to anyone using a packet sniffer. The following figure demonstrates this problem using Network Associates' Sniffer Basic 4.50.05 to capture packets from a computer running Windows 2000 Service Pack 4 and OE (Outlook Express) 6.

For a POP3 account, Sniffer 4.50.05 caught packets that contained both the username and the password. The following figure shows a portion of the packet capture:



As clearly visible in this figure, the Summary section of the packet capture displays the full username (with domain and extension appended) and the password. In the original packet capture, the username and password were pink to match the other text on the line. The author altered them to hide their actual values and to make them easier to identify. As seen in the figure, the protocol was POP3 and the port was 110, the common POP3 protocol port. The results are the same for IMAPv4 and Web-based eMail services.

Employee monitoring is a fiercely debated topic, and it is important for individuals to assume that their employer possesses the technological capabilities and legal right to read employees' eMail messages or monitor their Web access. According to Janice C. Sipior, Burke T. Ward and Sebastian M. Rainone, "As electronic communications grow in importance, so too has the need to address privacy issues in the management of E-mail systems. Because the legal system has not kept pace with the ethical issues accompanying the use of E-mail and there is no agreement on what constitutes a reasonable expectation of privacy, organizations must create their own internal policies" (41). Many companies now require their employees to sign documents describing in detail the organization's technology policies. Court cases have repeatedly upheld the right of companies to monitor and read their employees' eMail (42-43). Other cases have upheld the right of ISPs and other eMail providers to read transmitted messages

as well (AP "Court: E-mail"). This thesis will discuss additional problems related to eMail in the workplace in later sections.

Any HTTP (HyperText Transfer Protocol) transmission not protected by a secure session is susceptible to intrusion. One example of this is the login process to simple managed networking devices, such as cable modem routers. Cable modem routers manufactured by 3Com Corporation do not use a secure login by default and do not even offer the option of secure login. The authentication process for these devices transmits the password as plain text as part of a POST request. Crackers could use the login information to open ports in one of these routers, which are typically deployed by individuals or by SOHO (Small Office / Home Office) companies for their primary communications, and by enterprise organizations for their backup communication links.

The Problems of IP Addresses

IP addresses provide an easy method of determining an individual's physical location and identity. Many tools and Web sites are available that can trace an IP to the organization that is the authority to that address block, and possibly even to that IP address's geographical location. Law enforcement, government agencies and criminals could use or abuse geographical IP address information.

Determining an individual's IP address (and subsequently physical location) involves getting them to send you an eMail message or visit a Web page that you created. A typical eMail header includes the following information: Message arrival time (in UTC – Coordinated Universal Time), sender's return eMail address, text encoding, MIME (Multipurpose Internet Mail Extensions) type information, sending eMail application and message ID (in the format idNumber@sendinghost.tld). Also included is the subject, sender's name and eMail address, date

and time sent, date and time received, information regarding whether the message was forwarded from one mailbox to another (in the format ORCPT originalemail@originalhost.tld), sender's IP address, recipient's eMail address, recipient's IP address, and FQNs (Fully Qualified Names) for all servers directly involved in the transmission.

VisualRoute 7.0g (mentioned in the section regarding WHOIS lookups) is an exceptional program for geographically tracking IP addresses and determining information regarding the owner of the IP address. VisualRoute can query the end node using either an IP address or a domain name. The ability to resolve IP addresses to domain names (known as a "reverse DNS query") is an important part of determining the physical location of an IP address, as the originating domain for an IP address may end in one of the two character country codes, revealing the host's country of origin (Ankit Fadia "Getting geographical"). VisualRoute 7.0g also returns the time zone location of an IP address, providing more information regarding the location of the IP address.[4]

Web pages can gather browsers' IP address information using SSI (Server-Side Includes), JavaScript, or through the HTTP and FTP (File Transfer Protocol) logs, which keep detailed records of all requests for resources. These logs vary between server software packages, but generally contain the type of request, resource requested, location of the requested resource, time of the request and IP address that made the request.

Dynamic IP addressing is the method most commonly employed by ISPs (Internet Service Providers) for regular customers, including dial-up, cable modem and DSL (Digital Subscriber Line). The ISP assigns the dynamic IP address information (which may include IP

[4] For in-depth case studies on using VisualRoute to determine the geographical location of an IP address, see VisualWare's Web site at http://www.visualware.com. For a case study on using VisualRoute to determine the identity and geographical location of a hacker, see Sanders, Aaron D., "Utilizing Simple Hacking Techniques to Teach System Security and Hacker Identification".

address, DNS server IP addresses, gateway IP address and lease time) to the user's computer upon authentication to the ISP's network. The lease states the length of time a computer may retain the address information before it must request a new address. During the renewal process, the computer releases the address information and sends a renewal request to the server, in which the computer requests new address information. One problem with dynamic IP addresses is that they are often not dynamic. It is common for an ISP to assign a lease to a computer that is at least one week in length. In addition, the servers assigning the IP address information keep a log of IP address assignments that includes the date and time of the assignment, length of the lease, and date of the address' release. For these reasons, dynamic IP addresses are usually as easy to trace to the desired owner as static IP addresses. Numerous court cases have pitted ISPs against law enforcement officials attempting to retrieve a copy of their IP address assignment list for prosecution of a suspect. Many ISPs fight against orders to provide IP address assignment information in the interest of preserving their users' privacy.

The problems with TCP/IP and the WHOIS command are extremely dangerous, and increase the Privacy Level Indicator to 2.00. The only factor preventing a larger increase in the Privacy Level Indicator is that many current computer users are not familiar with WHOIS queries and IP address tracking. As pre-teen technology users move from elementary school to high school, the threat from these factors will increase. Society requires a universal solution to WHOIS privacy, because there is no reason for personal information in registration records. Unfortunately, the other issues are difficult to remedy, and will remain unsolved. The problems associated with the TCP/IP addressing scheme are inherent to the protocol's method of operation, and are virtually impossible to remedy.

Cookies: A Dangerous Treat

Cookies are small text files (usually no more than a few kilobytes in size) used by Web sites to store information on the local computer. Web sites usually utilize cookies to customize the site's layout to the user's preferences or greet the user by name. In the early days of eCommerce, Web Sites used cookies to track details such as a user's credit card number, username and password, and items added to their shopping cart, along with their layout preferences. Due to privacy and security issues involving cookies, their use to store personal information has declined, and session variables and database records have taken their place.

The majority of users select the same username and password combination for each site that requires authentication. Obviously, it is much easier to remember one username and password than it is to remember many varied combinations. Unfortunately, this enables an attacker to take advantage of the user by designing a Web Site that requires the user to provide a username and password. Once the user enrolls with the site, their username and password will be stored in the cookie on their computer or in a database on the server. Since the user probably uses the same username and password for every site that requires authentication, the site operator can attempt to use the user's username and password information on other sites, including shopping, credit card and banking sites.

Cookies have a much darker side of mischievous use. According to Michael Miller, "Cookies are typically used to serve personal information to you on return site visits; they can also be used by Web-based marketers to track your online behavior" (385). According to Miller, "Of late, however, a number of e-mail spammers have been using HTML e-mail to deliver cookies to unsuspecting recipients – and then using those cookies to track your online activities" (384). The use of cookies by marketers that participate in "advertising networks" has caused

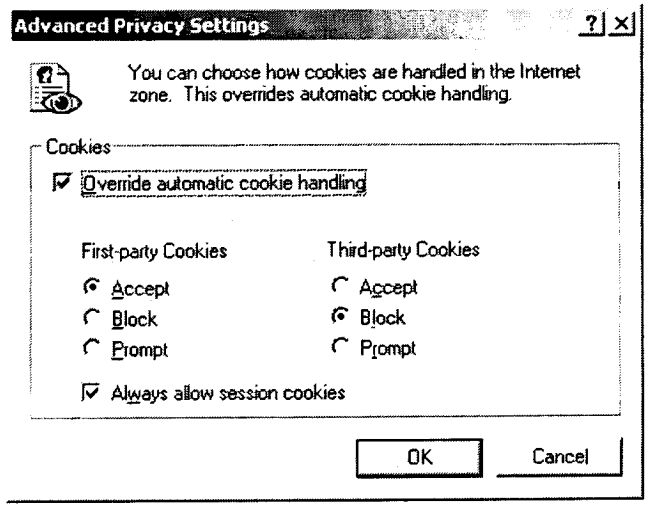
cookies to come under examination. In modern Web-based advertising, a few companies handle the ad placement and display services for most of the ads served to users. These companies are referred to as advertising networks because they specialize in marketing and advertising and they place ads for companies on multiple Web sites. Some of the largest advertising networks are DoubleClick, WebSideStory (Hitbox) and Atlas DMT. DoubleClick's history contains numerous accusations of privacy violations, in respect to the company's use of cookies and the personal information they collected from the user.

An organization can contract with one of these advertising networks to streamline the process of advertising on the Web. All of the mentioned advertising networks have developed tools to help organizations with the ad creation process, and have performed an enormous amount of market research, enabling them to select the best resources for their clients. For example, imagine that Toyota contracted with DoubleClick to place advertisements on the top three news sites read daily by Caucasian women in the 20-29 age bracket. The privacy issue is that if Toyota wishes to use the ads to place a cookie on the user's machine, the cookie's domain of origin will be that of the advertising network (DoubleClick), and not the organization that purchased the advertising service (Toyota). If two of the top three news sites were http://www.msnbc.com and http://www.cnn.com, the cookies from Toyota's ads on those two sites would belong to the domain DoubleClick.com, and originate from an address associated with DoubleClick. For this reason, DoubleClick can track users' movements around the Web by examining the cookies that they have placed on behalf of their partner organizations. DoubleClick can read all of the cookies that it has placed on a given user's machine for any of its partners (not just the ones for Toyota). The company can then offer to sell this information to its partners as part of an advertising package. From cookies that it has placed on a user's computer

of behalf of other companies, DoubleClick might determine that women of the previously mentioned demographic regularly view pages from http://www.womansday.com, and suggest that Toyota allow DoubleClick to place ads on that site.

Cookies can gather an unlimited amount of personal information regarding an individual, in addition to tracking a user's movements around the Web (hence the term "tracking cookie"). A user might have innocently signed up for a newsletter or filled out a form on a banner ad. Any information they entered into the form now belongs to the advertising network, which usually means that they will compile behavioral data and sell the information to all interested organizations.

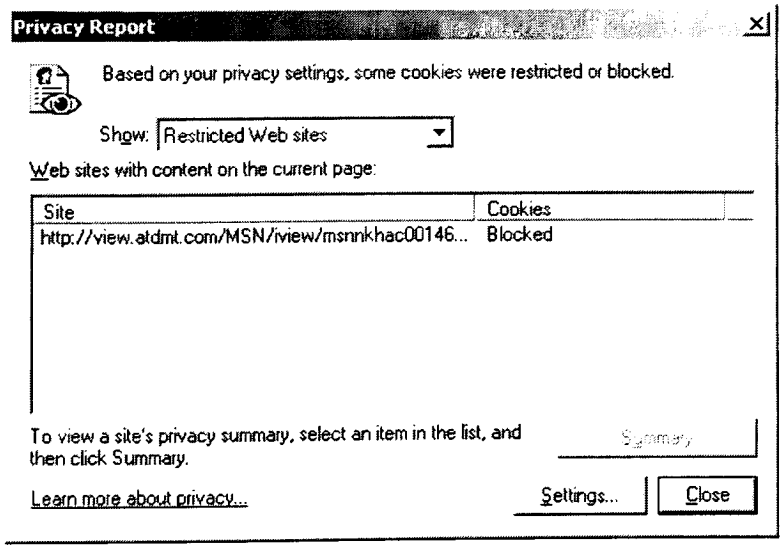
Verifying that cookies are indeed coming from one of the advertising networks is simple (as is blocking them) when using IE6, which has built in cookie handling capabilities. Clicking **Tools>Internet Options**, then the Privacy tab and finally the Advanced button will show the cookie handling settings on the user's browser. The following figure shows the displayed dialog box:



Checking the box to override automatic cookie handling allows the user to fine-tune their options for cookie handling. First-party cookies are the "good" cookies, placed on the user's

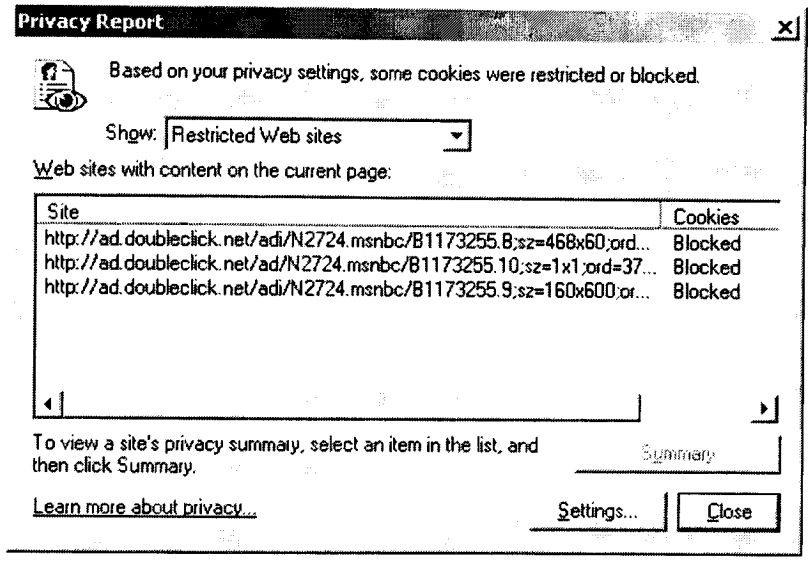
computer by the site they are currently viewing. Most sites utilize first-party cookies for the purpose of page customizations, such as local news, weather, and sports on MSNBC.com (http://www.msnbc.com) or the ability of Amazon.com (http://www.amazon.com) to identify the user without requiring user authentication. Third-party cookies are the "bad" cookies, placed on the user's computer by an advertising network. Blocking third-party cookies will rarely diminish the user's browsing experience. Most sites utilize session cookies for the legitimate purpose of maintaining the user's current session. Disabling session cookies makes shopping online very difficult and many sites will not work properly without them.

Once a user has blocked the placement of third-party cookies on their computer, they can easily verify that blocked cookies were from one of the advertising networks. When IE6 blocks a cookie, an icon of an eye with a minus sign below it appears in the lower right-hand corner of the browser window. Double-clicking on this icon will display information about the cookie that was blocked. For example, visiting http://www.msnbc.com causes the blocked cookie icon to appear in the specified area. Double-clicking on the icon brings up the following window:



As displayed in the figure, the blocked cookie originated from http://view.atdmt.com, yet none of the ads displayed on the MSNBC.com front page are for any company residing at that Web

address. The address http://view.atdmt.com is the domain used by the Atlas DMT advertising network when placing cookies on a user's computer on behalf of one of their partners. Double-clicking on a blocked cookie will bring up information regarding the cookie, the domain that placed the cookie and possibly that organization's privacy policy. Clicking on the blocked cookie in the figure confirms that Atlas DMT was indeed placing the cookie. The following figure shows the cookies blocked while viewing a story on MSNBC.com:



This figure shows three cookies that the domain http://ad.doubleclick.net attempted to place on the user's computer. The served Web page does not have any ads for an organization named DoubleClick, only uBid, Toyota, Newsweek and Compaq. The address http://ad.doubleclick.net is the domain used by DoubleClick to place cookies on a user's computer on behalf of one of their partners.

The EU, a leader in navigating the waters of privacy legislation, recently enacted laws to prevent spam and limit cookie usage. "Last July, the EU adopted a tough privacy regulation on electronic communications. It bans all commercial e-mail unless a recipient has asked for it. The regulation also sets strict rules for installing Internet 'cookies,' which hook a computer into a

Web site" (eWeek "EU Orders"). Asian and North American governments should follow the precedents set by the EU. Limiting the use of cookies is an important step in helping to protect users' privacy.

Spyware: Tracking your Steps

One of the most prevalent threats to anonymity on the Web is spyware. According to Webopedia:

> "Also called *adware*, spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers" ("spyware").

Some of the more prevalent spyware programs or companies include Gator, Comet Cursor, ClickTillUWin and Alexa. Gator is probably the most prevalent spyware program in existence today. According to Miller, "Its main function is to paste new pop-up ads over existing banner ads – thus hijacking ad space for their clients…To give you an idea of Gator's reach, the software sends an average of two pop-up ads per week to more than 15 million people – with most users not even knowing that it's installed on their systems" (368). Since most spyware programs are secretly bundled with other programs, users often do not know that the spyware program is installed and running on their computer.

Some spyware programs work by installing a BHO (Browser Helper Object) into IE (Internet Explorer). In some cases, the installation of a BHO causes the addition of a new toolbar

to IE. In many cases, the BHO will not make any visible changes to the user's system or applications, making it undetectable to the user. Once installed, the BHO can monitor the user's browsing habits, pages viewed, time spent on each page and search engine queries. Some spyware programs can even take control of a user's Webcam, turning it on without their knowledge.

One of the more insidious operations of spyware is keystroke logging. Some spyware programs install keystroke loggers on the infected machine, allowing the spyware's creator to record all of the user's keystrokes. Keystroke loggers provide the attacker with an ordered list of every key the user types. Attackers could use the data to determine passwords, financial information, credit card information and secret business or personal information.

Another operation of spyware is to enlist computers for spam mail campaigns. One recent report states that hijacked computers send 30% of all spam (Munir Kotadia "Hijacked PCs"). Other estimates are not so cautious: According to Sullivan, "Researchers say hundreds of thousands of vulnerable computers are being used to launch spam campaigns now. In fact, 70 percent of all spam is now sent this way, according to anti-spam firm Message Labs Inc. — and perhaps 6 to 7 billion spam messages are routed through hacked home computers" ("The secret"). Spammers often cannot transmit the massive number of eMail messages they send (reportedly around 500,000 messages per hour for successful spammers) from an account with one ISP without detection, so they use hijacked computers across the globe to spread the workload.

The debate over spyware has reached Congress, as legislators are debating how to handle the growing problem. The FTC (Federal Trade Commission) believes that additional legislation will only complicate the process of installing new software (MSNBC "Lawmakers vow").

However, Congress believes that the FTC is not working hard enough to stop the spyware epidemic, and spyware is too dangerous to address with a slow approach (MSNBC "Lawmakers vow"). Only time will tell if Congress can create a logical definition for spyware that will separate legitimate software from illegitimate spyware, without greatly complicating the software install process for end-users.

The threat from cookies and spyware is tremendous. These insidious threats lurk on the individual's computer, and therefore have the potential to track and record everything that the user does. Every key that the user types, every program they run and every Web site they visit could fall into the criminal possession. For this reason, it is necessary to raise the Privacy Level Indicator to 2.50. The threat from spyware cannot be understated, and is the most dangerous threat examined thus far. While persistent digital nyms and the panoptic sort often require a conscious effort by an individual to provide a piece of their panoptic information to at least one organization, the secretive nature of spyware allows it to gather information with little action on the part of the individual using the infected computer. Advances in spyware development are moving at a faster pace than spyware detection software, and show no signs of slowing.

The Wonders of Wireless

All types of wireless transmission are subject to capture and analysis, regardless of the specifics of their operation. Capturing wireless signals can be very easy, depending on the utilized signaling technology and the attention given to security in the implementation.

Although they provide a more flexible work atmosphere, wireless mice and keyboards also offer a potential compromise to a user's privacy. These wireless devices use radio frequency to communicate with the receiver. Although inexpensive, relatively simple and robust, radio frequency technology is also much easier to intercept than other wireless technologies, due to the

relatively wide angle of the signal transmission. While manufacturers of wireless keyboards and mice develop them to limit the distance that the signal can travel,[5] the signals risk interception in situations where close contact occurs, such as apartments, dormitories, computer labs and many work environments. Like the radio in a car and other broadcast transmissions, receiving wireless device transmissions does not require pointing the antenna directly at the source, as is required with point-to-point transmissions. Instead, the receiving antenna only requires placement in the air in an area that will receive the radio waves. In the case of wireless devices, this means that signal interception can occur within about ten feet in any direction from the device or the receiver. One can test this by moving a mouse and keyboard away from the receiver in different directions and different angles, testing the signal loss.[6] In addition, Logitech maintains a Web page that lists the radio frequency that every wireless Logitech device functions on,[7] making it much easier to intercept the signals. Cordless telephones are vulnerable to the same problems as wireless keyboards and mice, and it can be simple to intercept the transmissions between the phone and the base antenna. It is important to remember that with a cordless telephone, the telephone actually exists inside of the charging base connected to the wall by the phone cord. A cordless handset is very similar to a radio antenna, designed to capture the radio signals broadcast by the base. It is always interesting to walk around with a cordless handset, and observe just how far the signal will travel, through both open space and through physical obstruction. A typical 2.5 Gigaheztz (Ghz) cordless phone can cover the entire area of an average

[5] Logitech's basic iTouch Wireless Freedom keyboard works flawlessly up to approximately 6 feet. From 6 to 8 feet the keyboard functions, but experiences a slight delay before typed characters appear on the screen. The keyboard stops functioning past 8 feet. The results are similar for the mouse that accompanies the keyboard.

[6] Along with the distances previously mentioned, the Logitech iTouch Wireless Freedom keyboard and mouse used to type this thesis have no problem transmitting data with the keyboard or mouse pointed in the total opposite direction of the receiver.

[7] The English language version can be found at http://www.logitech.com/index.cfm?page=support/products/document&CRID=1796&contentid=4553&contentid2=5360&showalldocuments=0&countryid=19&languageid=1.

two story house. For these reasons, using a standard cordless telephone opens up the user to eavesdropping. Cellular telephones also suffer from many of the eavesdropping problems that effect cordless phones.

Wireless networks suffer from the same security and privacy problems as wireless mice, keyboards and cordless phones. Using a wireless network greatly decreases security and privacy, and it is important to take proper precautions to secure wireless networks. Minimally, unsecured wireless networks provide free Internet access to unwanted users through a practice known as "War Driving". In War Driving, a cracker drives around a neighborhood looking for unsecured wireless networks that they can use to gain free access to the Internet. By joining the wireless network, they gain access to all of the resources available to authorized users. In the worst-case scenario, unsecured wireless networks provide crackers with access to passwords, financial information, credit card information, private files and other resources not meant for public consumption. It is not uncommon for a home owner or apartment dweller to detect multiple unsecured wireless networks within range of their equipment.

The solution to wireless problems is encryption. Encryption protects a signal so that only the intended recipient can read the message. Only a few models of wireless keyboard support encryption from the keyboard to the receiver. Models supporting encryption are much more expensive than models that do not, and encryption is disabled by default, nor is the user strongly encouraged to enable the keyboard's encryption feature. Only the most expensive cordless phone models support encryption, although the number of phones that support encryption increases as the cost of implementing encryption rapidly decreases. Most cellular phones support encryption, although support for encryption in cellular networks is not widespread. Both components are necessary for a properly encrypted cellular system.

In terms of the Privacy Threat Indicator, wireless does not have a clear and obvious effect. The threats from wireless technologies raise the indicator to 3.00, because most individuals are not aware of the proper techniques for securing wireless communications, and many wireless security standards are still imperfect. At the same time, marketing campaigns have pushed wireless technologies into many homes and businesses. The key point is for wireless vendors to address the lack of awareness on the part of the consumer, and create wireless devices and technologies that are highly secure from their first activation. As awareness and technology improve, the threat from wireless communications should decrease. If these changes do not occur, the threat from wireless devices will increase proportionally to their market penetration.

Archiving

As technology advances and the cost per megabyte of disk storage decreases, archiving of data becomes common. Three often-archived resources that can reveal an individual's panoptic information are newsgroup postings, eMail messages and Web sites.

The functionality of Usenet newsgroups is very interesting, as almost every message ever posted to every newsgroup is contained in a public archive (now owned by Google, and accessed through http://groups.google.com). The Web-based front end to the archive enables searching through the postings based on a wide variety of search criteria, including post author. "The Smoking Gun" used the Usenet archives to uncovered incriminating messages posted years ago by current contestants on the CBS reality show "Survivor" ("More Sleazy"). The case study later in this paper will examine newsgroup archives further.

Organizations are increasingly archiving eMail, as proof of statements or actions. The recently passed Sarbanes-Oxley (Sarbanes-Oxley Act of 2002; H.R. 3763) legislation will

increase most organization's eMail archiving practices. The law requires detailed audit trails of publicly held companies' accounting, financial, and technological practices, including permanent archiving of all eMail messages. An unscientific poll conducted by Sunbelt Software found that 30.68% of respondents (197 votes) do not archive eMail, 14.48% (93 votes) archive eMail 0-6 months, 9.65% (62 votes) archive eMail 6 months to 1 year, 20.71% (133 votes) archive eMail 1-5 years and 24.45% (157 votes) archive eMail 5 years or longer ("Do You"). Other legislations and the threat of legal action have caused many ISPs and businesses to consider implementing eMail archiving.

Web sites have been archived since 1996 by The Internet Archive's "Wayback Machine". With the Wayback Machine it is possible to view nearly every version and update of a site since 1996, even if the site no longer exists at the URL (Uniform Resource Locator) specified. The Wayback Machine is very interesting from a historical perspective, allowing an individual to examine the changes in style and layout that a particular site followed through the years. As with newsgroup postings and archived eMail, the Wayback Machine also allows viewing of pages and statements from an individual's past that they might have been trying to forget.

eMail archiving should not effect the privacy level any more than the insecurity of the original eMail transmission. In fact, SOX (Sarbanes-Oxley) compliant organizations are required to record every instance of an individual accessing the organization's eMail archives, providing some sense of reassurance regarding eMail archiving. Worse are the archives of Web sites and Usenet posting. At this point, neither is threatening enough to raise the Privacy Level Index (since Usenet postings and Web sites are globally public in their original creation). However, we are guaranteed to see examples in the future where politicians or other public figures are embarrassed by archived messages from their past.

Information Gathered from the Local Computer

The previous paragraphs detailed methods of gathering information about an individual from locations that are remote to that individual and their property. It makes sense that since a large amount of information exists on remote and indirect sources, an even larger amount of information may exist on an individual's personal computer. Law enforcement agencies often confiscate an individual's computer during a criminal investigation. Some obvious sources of personal information (documents, pictures, eMail messages, receipts for online purchases) exist on an individual's computer and are generally easy to remove. However, much subtle and well-hidden information exists on an individual's computer that can provide many details regarding the individual. Although encryption programs (such as PGP) can protect visible information sources, these other subtle clues may be difficult to erase.

On a computer running Windows 98 or ME, the files Applog.log (\%windir%\Applog\Applog.log) and Optlog.txt keep a record of every application executed on that computer, the frequency of execution and the date and time of the application's last execution. Although the intended use of the file is to allow the Disk Defragmenter to better optimize the disk drive, the files could be very useful in logging information about an individual and their activities. Frequent use of a Visual Studio application (especially Visual Basic) could be evidence of an individual that practices writing viruses. Frequent use of a P2P (Peer-to-Peer) file sharing application could be evidence of a media pirate. Frequent use of photo editing or video applications could be evidence of a child pornographer. The files are created by the Task Monitor application, which is installed on every Windows 98 computer and (without user intervention) runs while the computer is power on, tracking application usage. Deleting the Applog.log file is only a temporary solution, as the Task Monitor will create a new file if it

cannot find an existing one. The only way to prevent the creation of Applog.log is to disable the Windows 98 or ME Task Monitor, which in turn reduces the effectiveness of the Disk Defragmenter. In Windows 2000 and XP, information regarding application usage is available through the "Add/Remove Programs" applet of the Control Panel. Windows XP contains a folder named Prefetch, located at %systemdrive%\Windows\Prefetch. This folder contains a list of the most often-used programs and drives, for use by Windows and Disk Defragmenter. As with the Applog.log file in Windows 98 and ME, information in the Prefetch folder could be used to determine information regarding the user's habits.

Many companies install software packages on their users' computers and servers to determine what programs the user executes on the computer, usage frequency and usage duration. These monitoring programs have many legitimates uses, including license enforcement and determining which programs are most popular and which are rarely or never used. This information enables companies to make better judgments in their future purchasing decisions. However, usage data also provides companies with the ability to profile the interests of their employees, as well enabling them to create a detailed analysis of the amount of time an employee spends working.

Starting with Windows ME and continuing to Windows XP, Microsoft has implemented the ability roll the system back to an earlier date. Although previous versions of Windows allowed the user to roll the Registry back to an earlier date, the ability to roll most of the system back to an earlier date and recover any lost data or settings is a major change. While the System Recovery feature could enable a user to recover data in the event of a loss or accidental deletion, it also enables the recovery of data that the user may have been trying to destroy.

By default, each individual installation of Windows Media Player 9 contains a unique player ID that identifies each individual installation and user. Considering that by default Media Player 9 contacts Microsoft and Atlas DMT every time it starts, the use of a unique ID is unnerving. Thankfully, it is possible to configure the application to prevent it from contacting Microsoft and Atlas DMT, and spyware removal programs can delete the unique ID from the system registry.

In addition, Media Player maintains a media library, which keeps a very detailed list of all media ever played by the player. The Media Library can be accessed through a button on the left side of the player's navigation menu. The first category in the Media Library is the Now Playing list, which contains a list of the media currently playing. Every item on the Now Playing list is also contained in its respective category in the library (music or video).

The All Music category contains three sub-categories: Artist, Album and Genre. The All Music category contains the following information about every audio file played on Media Player 9: Title, artist (if embedded in the file), album (if embedded in the file), rating, Media Info, Genre (if embedded in the file), Length, Bitrate, Type (.mp3, .wav, .wma), Acquisition Time (last time the song was played), and the File Name. Songs played from the legal retail copy have the designation "(retail)" beside their album name. All other copies have no indication towards their status, but the absence of the "(retail)" designation conveys plenty of information about their origin. This information is a treasure trove for Microsoft, marketers and law enforcement officials.

The Artist sub-category displays a list of all authors embedded in played audio files. Double-clicking on an artist's name reveals all of that artist's songs played on the player (with all of the information contained in the All Music listing).

The Genre sub-category displays a list of all genres embedded in audio files. Double-clicking on a genre reveals all of the songs played on the player from that genre (with all of the information contained in the All Music listing).

The All Video category is constructed similar to the All Music category, with sub-categories for Actor and Genre. The attributes recorded for each video file are the same as those recorded for every audio file. The Actor sub-categories lists all video files which had an actor embedded in them, and the Genre sub-category lists all videos that had a genre embedded in them.

The My Playlists category lists all playlists played on the player.

The Radio category lists all radio stations streamed to the player.

Minimally, the information gathered from Windows Media Player 9's Media Library provides plenty of information regarding the individual's listening and viewing habits and tastes. It could also tell a lot about the legality of the media consumed by the user. If an individual is concerned about information contained in the media library, right-clicking on a file and selecting Delete From Library allows an individual to delete the listing from the library, as well as from their computer (if they choose this option). The Options menu in the player can also clear this information. On the Privacy tab, there are buttons to clear all of the media in the Media Library.

The Options menu also contains checkboxes that allow the user to increase the privacy of the player (contained on the Privacy tab). Included are the ability to prevent the player from sending its unique ID to content providers, and the ability to prevent the player from sending usage data to Microsoft.

In the case of Windows Media Player 9, it appears that physical access to the local computer might not be necessary in order to view a user's Media Library. On June 25, 2003

Microsoft released "Microsoft Security Bulletin MS03-021: Flaw In Windows Media Player May Allow Media Library Access (819639)", and then updated the release with new information on July 4, 2003. According to the Microsoft TechNet bulletin:

> "An ActiveX control included with Windows Media Player 9 Series allows Web page authors to create Web pages that can play media and provide a user interface by which the user can control playback. When a user visits a Web page with embedded media, the ActiveX control provides a user interface that allows the user to take such actions as pausing or rewinding the media. A flaw exists in the way in which the ActiveX control provides access to information on the user's computer. A vulnerability exists because an attacker could invoke the ActiveX control from script code, which would allow the attacker to view and manipulate metadata contained in the media library on the user's computer" ("Microsoft Security").

A Web page that combines an embedded media clip with a correctly written ActiveX script would allow an attacker to compromise the Media Library on an unpatched system. The vulnerability makes it much easier for law enforcement or a cracker to gather information regarding the user. In addition, the attacker has the ability to manipulate the data in the Media Library, allowing them to add or delete entries to the Media Library, potentially framing the individual for crimes not committed. The flaw may also allow an attacker to gain knowledge of the current user. According to the TechNet bulletin, "The attacker might also be able to determine the user name of the logged-on user by examining the directory paths to media files" ("Microsoft Security").

It is only fair to note that Microsoft is not the only company to experience problems with its media player. RealNetworks, creator of the once popular RealPlayer streaming media player, has had many problems with its media player, ranging from privacy violations (sharing user data

without consent) to allowing improper access to the local computer. One vulnerability enabled an attacker to hijack the local machine and gain full access rights equal to the current user.

Media applications like Windows Media Player, RealNetworks RealPlayer and MediaMatch Jukebox retrieve their media information (and in applicable cases perform their privacy violations) by contacting CDDB (http://www.gracenote.com/). CDDB (now known as GraceNote) maintains a user updatable database of nearly every professional audio recording ever made. The company sells the information it gathers from media players to organizations interested in utilizing the data for marketing purposes. For this reason, unique player IDs and privacy violations are a serious matter. The information transmitted to CDDB varies by application. For example, Easy CD Creator contacts CDDB's database to generate playlist information for CDs before copying. During the query, Easy CD Creator provides CDDB with its application name and version number. Disabling Media Player's unique ID greatly reduces the threat from a query to CDDB's database.

Microsoft's popular Messenger chat program is also open to attacks. According to Michael Kanellos, "The vulnerability in MSN Messenger versions 6.0 and 6.1 could let an attacker view the contents of a victim's hard drive during a chat session with the victim" ("MSN Messenger"). The attacker can retrieve and view files on the victim's hard drive without their consent. If the attacker finds files containing the victim's passwords or financial information, then identity theft is almost certain to follow.

Microsoft Word contains a feature called Track Changes that allows an individual to send a document to multiple recipients for editing. The individual monitoring the document's progress can then implement suggested changes into a master copy of the document with ease. The problem is that many features of Word, including the Track Changes feature, store metadata

regarding the document. Users can edit some of a document's metadata properties by clicking **File > Properties**. Available metadata for a Word document includes title, subject, author (by default the registration name for the Word installation that the document was created on), keywords, comments, date created, date modified, last date accessed, user that last saved the document (by default the registration name for the Word installation that the document was created on), revision number and total editing time.

When utilizing the Track Changes feature to manage a document's progress, the metadata includes information regarding previous versions of the document. The SCO Group, Incorporated discovered the effects of this feature when changes were uncovered in some of their legal documents. According to Stephen Shankland and Scott Ard, "The SCO Group filed lawsuits this week against DaimlerChrysler and AutoZone, but the Unix seller's attorneys also had prepared a complaint against Bank of America, according to a document. A Microsoft Word document of SCO's suit against DaimlerChrysler, seen by CNET News.com, originally identified Bank of America as the defendant instead of the automaker" ("Hidden Text"). SCO's legal team did not realize that the metadata created by the Track Changes feature existed, and it provided a glimpse into the company's thought process in determining the targets of its lawsuits. According to Shankland and Ard, "In the case of SCO's lawsuit against DaimlerChrysler, the Word document identified Bank of America as a defendant until Feb. 18--at 11:10 a.m., to be exact. The location for filing the suit also was switched from Bank of America's principal operations in California to Michigan, DaimlerChrysler's home state, on Feb. 27" ("Hidden Text"). In addition, flaws affecting the local user may originate from a server the user is connecting to, rather than on the user's computer. A flaw in Microsoft's Exchange 2003 eMail server software allows improper file access. According to Matthew Broersma, "The bug appears to affect an

Exchange component called Outlook Web Access (OWA), which allows users to access their in-boxes and folders via a Web browser. Consumers logging into their Web-based mailbox sometimes find themselves accessing another user's account, with full privileges..." ("Exchange flaw"). Allowing a flaw that is as fundamentally erroneous as this one is a major embarrassment for Microsoft. Rather than requiring the intruder to explore the system to find its weakness, this Exchange 2003 flaw directs the user to other folders on its own.

Most computer users do not realize that deleting files from their hard drive does not permanently destroy them. Computers organize their hard drives like a book, with a table of contents pointing to the corresponding content. Deleting a file does not remove that file from the drive. Instead, the OS removes the file's entry from the table of contents, know as the FAT (File Allocation Table) or the MFT (Master File Table). Computers, being rather unintelligent devices, normally do not know how to retrieve data once they remove the corresponding entry from the FAT. However, freeware and commercial programs are available that can recover or "undelete" previously deleted files. A computer only permanently deletes files when they write a new file in the same storage location that contains the old file. Even then, professional data recovery companies possess special equipment that can usually recover the original file.

Drive erasers are software applications that solve the problem of data deletion. When a drive eraser deletes a file (knows as "wiping"), the program writes a special sequence to the selected area that will minimize data recovery. Most drive erasers operate in conformity with a specification on proper data destruction put forth by the DoD. This specification details how to destroy sensitive data without harming the drive. For data of extreme sensitivity, the only way to guarantee data destruction is to use a drive eraser to wipe the drive, then physically destroy the drive's platters with a hammer, drill or through incineration.

One recent study found that drive sanitization practices are varied, but lean towards being careless rather than cautious (Abhi Shelat and Simson L. Garfinkel). In their study, Shelat and Garfinkel purchased hard drives from the secondary market (mostly from eBay) and examined the drives' contents for readable data. According to Shelat and Garfinkel, "Of the 129 drives that we successfully imaged, only 12 (9 percent) had been properly sanitized by having their sectors completely overwritten with zero-filled blocks; 83 drives (64 percent) contained mountable FAT16 or FAT32 file systems. (All the drives we collected had either FAT16 or FAT32 file systems.) Another 46 drives did not have mountable file systems" (24-25). They discovered one drive used in an ATM machine that still included 2,868 account numbers, dates of access and account balances (25). Approximately 42 of the examined drives contained recoverable credit card numbers (25). Their study emphasizes the critical importance of properly sanitizing drives before their disposal, reuse or resale.

The following scenario reinforces the importance of properly wiping disk drives before disposal. A company in Rochester, NY (New York) disposes of used computer equipment, donated by individuals and organizations in the area. The organization once received a server marked for disposal by a local school district. The school district did not wipe the hard drives before disposing of it. Being interested in information security, the organization's employees decided to attempt to view the data on the server's disk drives. The server had a RAID 5 (Redundant Array of Inexpensive Disks) disk array, so it would have been extremely difficult to read the disks by simply placing the drives in another computer. Since the server was running Windows 2000, the employees reset the Administrator password using Passware's Password Recovery Kit 6. Once logged in, the employees attempted to recover any recently deleted data

using Norton Utilities. The server had been the district's student eMail server, and Norton Utilities recovered all of the archived messages. The employees then properly wiped the drives.

For confidential drives, the minimal procedure is to format the drive, wipe the drive, then physically destroy the drives platters by drilling holes through them or breaking them with a hammer. Individuals concerned with sanitizing drives from their home computers should format the drives, then erase them to DoD standards. The most popular drive eraser program is Eraser 5.7, available from http://www.heidi.ie/eraser/default.php.

The threats posed by the Windows OS and various Windows applications are numerous, and a number of groups have suggested a migration to other OSes. However, most Windows flaws are preventable through regular use of the Windows Update site. As a result, software flaws raise the Privacy Level Indicator to 3.25. While it is necessary to increase the Privacy Level Indicator, it is difficult to justify an increase greater than ¼-point. Users are migrating to newer OSes at a higher than anticipated rates, and newer OSes automate many of the tasks that are necessary for system security. Awareness of security issues is improving, and many new vendors have entered the security market. An increase in the Privacy Level Indicator greater than ¼-point would place OS flaws on equal footing with persistent digital nyms and wireless technologies, which they are not.

Available Information Section

The Wallet as a Tracking Device

One of the easiest ways to gather information regarding an individual is through the acquisition and subsequent usage of items contained in their wallet. Most individuals do not realize how often they are directly providing information to other sources.

The most common and most damaging item in the wallet is credit cards, including gasoline and store cards. During the initial application for a credit card, an individual provides information to the potential creditor. Although this personal information describes the individual applying for credit, the credit card company considers themselves the owners of the information provided in that specific transaction, because it involves them receiving payment (personal information) in return for the provision of a service (a credit card, pending the individual's approval).

When a credit card company approves an individual for credit, they enter all of the individual's personal information into a database maintained by the credit provider. Credit providers believe that the information is theirs to use as they please, in accordance (or occasionally in violation of) their privacy policy. In almost all cases, this means that a credit provider will sell all of the information it possesses regarding each customer to as many of its partners as possible. Modern technology enables an effortless transfer of information, as a creditor simply needs to transfer all of their customer records to CD (Compact Disc) or provide access through an electronic interface. The sale of data causes the telephone calls, eMail messages and postal mail letters from telemarketers, offering an unimaginable array of goods and services.

The problems with credit cards do not stop with the sale of personal information, as credit cards can leave an audit trail describing an individual's lifestyle. Details might include their store preference (brick and mortar or online), travel habits (where, when, how long and the route traveled), spending habits, hobbies and interests, and their needs, wants and desires. Credit card purchases show the amount of the purchase, items purchased, and the date and time of the purchase. Individuals should be concerned about the information generated by credit card

transactions and maintained by the credit provider. The volumes of information that credit providers possess regarding an individual paints an amazing picture of the individual's personal characteristics, and provides plenty of useful information to companies willing to pay the credit provider's fee. It should not be surprising that organizations conduct credit checks before granting credit to an individual, for job applications and for rental applications.

Another interesting card is the one provided by Jillian's, a national chain of "adult fun centers". An individual can partake in the following activities at a typical Jillian's location: Bowling, billiards, numerous video games, darts, air hockey, foosball, eating and drinking. To play a game at Jillian's, one must acquire a Jillian's card and place money in the account that is associated with the card. Every game in Jillian's has a card reader, which automatically deducts the cost of that particular game from the player's account. When the player's account no longer has enough money to play any games, they can have an associate "replenish" it, using standard forms of payment.

The problem with the Jillian's card is that every card reader is a networked device, which stores account information in a database. Information recorded includes games played, time, date and location. In this way, an individual's playing habits, frequency and types of games played could be determined by gaining possession of their card, or breaking into Jillian's information database. There is no doubt that the government, employers, or insurance companies would love to know if a suspected terrorist, murderer, or employee regularly played games that involve shooting and violence. Plenty of anti-violent gaming organizations would also be interested in the information available from Jillian's database.

One of the more prevalent methods of gathering panoptic information about an individual is through "dumpster diving", in which one individual searches through another individual's

waste in search of tidbits of information. Dumpster diving ranges from common theft from an individual's garbage can to large-scale corporate espionage. Larry Ellison, CEO of Oracle, once hired someone to search through dumpsters belonging to rival Microsoft in search of secret information regarding Microsoft's oft-criticized business practices. Thieves often pose as homeless people searching through dumpsters looking for food, when they are really searching for discarded financial information to use for fraud purposes (Garfinkel 30). This is a threat regardless of whether you actually place your refuse in a dumpster, as garbage cans are equally vulnerable to invasion. Preventing dumpster diving simply requires destroying any information that might be of use to anyone else, minimally by using a cross-cut paper shredder.[8]

For these reasons, it is important to shred any documents relating to credit cards or personal financial information. Statements vary between card issuers, but it is safe to assume that all statements will contain the full credit card number, credit card type and mailing address of the cardholder. Equally dangerous are the unsolicited credit card offers that most individuals regularly receive in their mailboxes. These offers often come with all of an individual's personal information pre-filled, including their SSN. Throwing these offers away without shredding them first is dangerous. When considering what documents to shred, always err on the side of safety and privacy rather than being lax.

It is also very important to examine receipts for any goods paid for with a credit card, as they sometimes contain the complete billing information. In addition, just because one store in a chain displays certain pieces of credit card information on a receipt does not mean that all stores in the chain will display the same information. Franchises generally give freedom to their franchisees in the selection of their financial suppliers, as well as the specific settings of the

[8] Incineration is probably the best way to dispose of unwanted documents, although access to a place to burn is difficult, especially considering laws regarding burning and pollution.

credit card machine they select. In addition, when paying by credit card, it is important to examine both copies of the receipt. In many cases, a store will place the entire credit card number on the store copy, but place only the last four digits on the customer's copy. This is very dangerous and impractical. All this does is gives store employees the opportunity to steal the customer's credit card information from the receipt and use it later for their purchases. The following table displays a small sample of stores in the Rochester, New York area and the information they place on their credit card receipts:

Store	Location	Card Type	Account Number	Expiration Date
Subway	Henrietta	No	Full	Yes
Barnes & Noble Booksellers	Pittsford	Yes	Last 4 digits	No
Tops Markets	Henrietta	No	Last 4 digits	Yes
Big Lots	Henrietta	No	Last 4 digits	Yes
Office Depot	Henrietta	Yes	Last 4 digits	No
Target	Henrietta	Yes	Last 4 digits	No
Old Navy	Henrietta	Yes	Last 4 digits	No
Atlanta Bread Company	Henrietta	Yes	Full	Yes
Subway	Henrietta	Yes	Last 4 digits	No
Subway	Henrietta	Yes	Last 4 digits	No
Wegmans	Henrietta	No	Last 4 digits	Yes
Tully's Good Times	Henrietta	Yes	Full	Yes
U.S. Postal Service	Henrietta	Yes	Full	Yes

Ruby Tuesday	Henrietta	Yes	Full	Yes

All receipts require shredding, even ones that contain only partial information. A thief will probably retrieve multiple receipts from the garbage at one time. By comparing the information contained on each, the odds are very good that they will be able to gather the complete information for at least one card. However, not all retailers are guilty of endangering their customers' privacy. In one instance, the International House of Pancakes restaurant, located at 2190 North Goodman Street, Rochester, New York 14609-1043, temporarily provided customers with the "restaurant copy" of the receipt, because it was printing with the customer's complete credit card information, and the "customer copy" was not.

The Dangers of Public Records

Public records have long been dangerous due to their availability, but before the Web, their danger was limited, because retrieving a public record often meant traveling to the physical archive where the record was stored. With news and gossip organizations battling each other to see which one can ruin more people's lives, information gathered from a public source becomes digitalized and made globally available in minutes. The Smoking Gun (http://www.thesmokinggun.com), a popular news site on the Web, has used public records and the FOIA (Freedom of Information Act; 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048) to uncover documents regarding many famous individuals. The Smoking Gun scans the documents and places them on the organization's Web site, where they are available before the entire world. In addition, the site contains copies of arrest photographs of famous individuals taken during their booking for crimes. In the modern world, one mistake can cause embarrassment and harassment on a global scale.

Public facing Web Sites are also a source of information. Higher education institutions, which should be especially careful with data because of FERPA (Family Educational Rights and Privacy Act; 20 USC §1232g), often place their students' information in public view, especially when celebrating their students' achievements. Pages listing honors students, Dean's List students or recent graduates often contain information ranging from eMail address and city of residence to full phone number and address.

The biggest problem with public records is that as the government and private industry become more interested in knowing everything that they can about a given individual, information brokers will offer to perform a panoptic sort on the various existing data sources and combine them together to provide a complete picture regarding a given individual. A partial list of information brokers includes LexisNexs (http://www.lexisnexus.com/), ChoicePoint (http://www.choicepoint.com/), Intelius (http://www.intelius.com/), US Search http://www.ussearch.com/consumer/index.jsp) Hoovers (http://www.hoovers.com/free/) and GuideStar (http://www.guidestar.org/). The information these companies can retrieve includes name, address, phone number, age, SSN, property information, criminal check, background check, death records, marriage records and divorce records. Hoovers provides business information, although if the business is a sole proprietorship or partnership, the query may return the home address and telephone number of the proprietors. GuideStar provides information about non-profit organizations, including their tax returns and financial statements.

Name Seeding

One way to track the usage of your personal information is through the "seed name" technique (Garfinkel 180). With name seeding, an individual uses slight variations of their name or address for the various catalogs, magazines and mailing lists they request. For example, an

individual might use their middle initial for one magazine, one without the middle initial, and another with a misspelled last name. When they receive unsolicited junk mail, they can examine the address label to examine the form or spelling of their name or address, thereby determining what source provided their information to the bulk mailer. While this does not enable an individual to prevent information sharing, it does provide them with the knowledge of what organization is sharing their information, allowing them to consider canceling their subscription with that company.

The amount of available information will only increase over time as database utilization increases. Individuals should be very aware of the contents of their wallet, and leave their Social Security card at home. In addition, they should not carry more credit cards than they need. The issue regarding public records is a difficult one, as the blame belongs to government agencies and organizations that individuals have no control over. Any organization dealing with an individual's panoptic information must be extremely diligent with that information, especially when storing it electronically. Publicly available information presents a dangerous threat to individual privacy, and raises the Privacy Level Indicator to 3.75. Most individuals have credit or debit cards, and use them often. In addition, most individuals do not understand the necessity of shredding documents that contain even the smallest amount of financial information. The ubiquitous existence of credit and debit cards, the high percentage of individuals that carry their Social Security Card, and the lack of education regarding proper disposal of financial information provides justification for the ½-point increase in the Privacy Level Indicator.

Case Study

Case Study

The purpose of this case study is to provide a concrete example of the amount of panoptic information readily available in databases worldwide. In addition, this case study provides examples that support the previously discussed changes to the Privacy Level Indicator. Viewing actual panoptic information retrieved from a small-scale panoptic sort reaffirms the danger of the many threats to individual privacy.

When attempting to uncover panoptic information describing an individual, one generally has a few pieces of information as a starting point. This information could include their true name, persistent digital nym, a username, phone number, eMail address, employer, educational institution, Web Site address, or home address. One can gather information from a variety of sources, including eMail messages, signature text on eMail or newsgroup postings, personal Web Site, conversation, phone book, instant messaging chat, or online message board postings. Using this information as a starting point, one can then begin their search for information regarding the individual.

This case study gathered its information from publicly available sources, without purchasing any information from a broker. One can purchase a large amount of information from one of the many information brokers throughout the world. In addition, information is increasingly available from more "reputable" sources, such as ChoicePoint or LexisNexis.[9] This information often includes the individual's SSN, address and telephone number, background check, criminal record and employment history. Information brokers have existed for decades.

[9] The reputation of any organization that collects and sells personal information, regardless of their practices and who they sell the information to, should be called into question.

However, technological advances have enabled greater levels of information collection and sharing.

Consider an individual represented by two persistent digital nyms. To protect the individual's privacy, we will call them "nymA" and "nymB". nymA was known at the beginning of the search, as was the address of the individual's personal Web Site and true name. The Web Site of nymA contains plenty or worthwhile information. The first relevant piece of information is a picture of nymA smiling and wearing a suit. The Alternate Text for the image describes the image as a "picture of nymA wearing a suit". The site is hosted on a Time Warner free hosting site, possibly signaling that nymA does not have the money or resources to host the site through a provider. One the front page, we are greeted by a message from nymA, which includes a new email address used by the persistent digital nym. According to the messages, nymA has recently learned to use Adobe Photoshop 7.01, Macromedia Fireworks MX 6.0, and is planning to digitize some videos using Adobe Premiere 6.5. The site also contains information regarding nymA's level of education, career aspirations, hobbies and interests, as well as a containing a copy of the individual's résumé. The site mentions that nymA is an avid video gamer, and holds numerous world records. The site details a number of nymA's beliefs, including those on code validation and site accessibility. The site also contains a Privacy Policy, and details nymA's beliefs regarding privacy.

Using VisualRoute 7.0g to analyze nymA's personal Web Site uncovers some very interesting information. The first interesting piece of information is that VisualRoute 7.0g was able to trace nymA's domain name. The WHOIS reply from nymA's domain contains the address and phone number for the domain's administrative contact, whom happens to be the same nymA that is the subject of this case study. With the popularity of the Web, and the

increasing number of people who desire to register a domain themselves, the information contained in the WHOIS database is extremely dangerous. The WHOIS record often contains an individual's home address and phone number, if they registered the domain themselves.

A search on Yahoo! for "nymA" returns eight results, three of which refer to the individual's persistent digital nym. From these results, an individual could determine that nymA authored two papers published in peer-reviewed journals, and determine the title, volume and publication date of each. In addition, the search results show that nymA had a fantasy drum corp, which finished in 10th place of the Fantasy Drum Corps International (FDCI) tournament in an unknown year.

Of the five results that were false positives, three referred to individuals that died before the nymA in question was born. The other two results provided some interesting information of their own. One is from the University of Notre Dame, and is a listing of all sophomores with last names beginning with the letters M-Z who are members of that university's Arts & Letters Science Honors program. While it does not refer to the nymA in question, the page does provide the last name, first name, college, major, address, phone number and eMail address of its nymA, along with the thirty-three other people that are a part of that group. This is an incredible amount of public information for a university to provide regarding its students, most likely without the students' consent. The final false positive is a Marine Corps promotion listing, which includes the individuals' name and the last four digits of their SSN.

A newsgroup search for nymA returns 87 results, all of which refer to the nymA in question. The first piece of information gathered from these postings is that the person represented by the persistent digital nym of nymA was active in posting messages, from June 6, 1997 to July 2, 2002. It is very easy to connect the postings to the same nymA, as they were sent

from the same email address, which was valid at the time for the nymA in question. It appears that nymA was unaware of the automated spiderbots that crawl through newsgroups, extracting eMail addresses from postings and adding them to spam mailing lists. Otherwise, nymA would have used a fake or altered email address in nymA's postings. Over time, nymA adds a signature tag to each posting, containing at first the nym, then adding a Web Site address, then adding quotes from famous philosophers, and finally adding industry certifications that nymA had earned. Since the signature adds to the foundation of the persistent digital nym, one only needs to associate any one of the postings to the nymA in question.[10]

One can gather a very large amount of information from these postings: nymA is a fan of the Atari video game systems and has ordered some games from a company named O' Shea Ltd. nymA is a very devoted fan of the band Queen, having posted many messages relating to them personally and their music. nymA is a fan of snowmobiling, having once gone 100 Mph (Miles per hour) on a Ski-Doo Mach Z snowmobile. nymA is apparently a fan of the Beach Boys, having posted several messages mourning the passing of Beach Boy Carl Wilson in 1998. nymA apparently was a fan of HP (Hewlett-Packard), having owned an HP 5PSE scanner and an HP 6020EP CD writer connected to a laptop. nymA is a fan of the bands Dream Theater and Rush, and loves hearing their music played on television during sporting events or other coverage.

In 2000, nymA had tickets for a Dream Theater concert in Pittsburgh that nymA was trying to sell for $24 apiece. The show unexpectedly was 21 and over only, and according to the post nymA was not 21 years old at the time. In June of 2000, nymA had trouble with an Abit VT6X4 motherboard with a Pentium III 667EB processor running Windows 98SE. Even after

[10] This is not entirely true, as someone could be posing as nymA, copying the basic signature style from other postings. An analysis of the body of each posting shows that the grammatical style is consistent in each posting, something that an expert could certify. We shall discover later that nymA eventually started using PGP to digitally sign all messages, which is a stronger guarantee of their authenticity, but also adds a surer layer of tracking to the persistent digital nym.

downloading the shutdown patch, the machine still would not shut down properly. The core voltage on nymA's PIII CPU (Central Processing Unit) was 1.6V. Later, we find more details of that system: A Maxtor DiamondMax Plus hard drive running on a Promise Hard Drive controller, a SoundBlaster Live! Platinum sound card, a Creative Labs Annihilator2 video card and an Encore 8X DVD drive. nymA seems knowledgeable regarding computers, posting a fair number of messages relating to troubleshooting and configuration issues. nymA does not like Hollywood Records, promising not to purchase anything from the company. nymA has been to the Rock and Roll Hall of Fame, and viewed articles of clothing from many of nymA's favorite artists.

nymA apparently does not hold a favorable opinion of the A+ Certification test. nymA appears to side with nVidia in the video card wars, complaining of the presence of 3dfx zealots in nVidia newsgroups. We later discover that nymA is not a fan of the A+ Certification book by Mike Myers. A fake Web page tricked nymA into thinking that a drunk driver killed the drummer for the Dave Matthews Band. nymA once had an HP 970 DeskJet printer that would occasionally print nothing but ASCII characters across the page. Professional wrestling's Ted DiBiase, the "Million Dollar Man", inspired nymA as his signature at one point contained many religious quotes from the wrestler turned public speaker. nymA apparently had plenty of trouble with an Asus A7A266 motherboard, as there are many posts relating to issues with this product.

The purpose of reprinting some of this material is not to bore, but to prove a point: The newsgroup archives can contain a vast amount of information about an individual, depending on the frequency and content of their posts. The information repeated in the previous paragraphs is simply extracted facts and quotes that any person could obtain legally from the Google archives. The posts are timestamped with the day, month, year and time of the posting, providing a

timeline of nymA's experiences in cyberspace. Anyone with training as a profiler or psychologist could probably construct a thorough profile about someone from this information.

Amazon.com is no less informing, especially if a user has created a wish list, baby registry or wedding registry. Any of these lists are searchable by an individual's name, and minimally provide more information regarding a person's life, and can provide personal details, depending on the content of each list. A search for Wish Lists created by nymA turns up seven results. One of these results lists the same town as where the nymA in question was born, which was determined from nymA's Web Site. Thus far, it seems like a match. A quick perusal of the items in the Wish List confirms that the items are definitely along the interest lines of the nymA in question.

The Wish List of nymA contains plenty of interesting information. One of the most interesting facts regarding Amazon.com Wish Lists is that the timestamps marking an item's addition to their Wish List greatly enables an observer to examine their growth of knowledge and interests. On September 7, 2001, nymA added seven trance, relaxation and instrumental CDs to the Wish List. It seems evident that around this time nymA discovered this genre of music. In October 2001, six DVD movies and concert videos were added to the Wish List, signifying a new interest in DVDs. Perhaps the true name behind nymA had a DVD player. Numerous books on AI (Artificial Intelligence) and philosophy appear on the Wish List during October and November of 2001. Authors include William A. Stubblefield, George Boole, George Luger and Ivan Bratko, all of whom are well respected experts in artificial intelligence and machine learning. Also listed are a numerous versions of Aristotle's "Physics" and a translation of Friedrich Wilhelm Nietzsche's "Thus Spoke Zarathustra". Also added to the list at this time were numerous books by the spiritualist Aleister Crowley, and Anton Szandor LaVey, known as the

father of the modern Church of Satan. It appears that perhaps nymA was into all various forms and manners of philosophy. Also from this period are many books by Issac Asimov (including "I, Robot" and a guide written by Asimov on the Bible and Shakespeare), DVDs containing "Transformers" episodes, a Britney Spears wall calendar, a CD by Jewel, a number of classical music CDs, and a Christmas CD by Christina Aguilera.

In January 2002, we see Henry Bieler's "Food is You Best Medicine", signaling that perhaps nymA was searching for dieting or health advice. On July 10, 2002, there are a number of cordless phones added to the list, signaling that perhaps a phone purchase was on the horizon. In October 2002, we see the classic "Design Patterns". In November 2002, nymA added books on Adobe Premiere, signaling that perhaps nymA was planning to do some video editing. At the beginning of 2003, some intensive theory books appear on the list, beginning with a book by Milton L. Mueller on the DNS system; a book on converged network architectures; a number of books on intellectual property and cyberspace law; and many books on swarm theory, chaos theory and emergence. The newest item on the list is a VHS version of the classic movie "Cloak and Dagger". From the Wish List, you can find a link to all reviews written by nymA, and learn that nymA has much respect for Bouhrez A. Fourazan, and very little respect for Clifford Stoll.

Not only are the products on Amazon.com lists revealing, but an individual can choose to put plenty of personal information into their profile, including date of birth, physical description, eMail address and comments for products added to the list.

Over time, the true name behind nymA developed a second persistent digital nym: nymB. Determining the second nym and connecting the two nyms to the same person is actually very simple, and requires only searching for nymA's eMail address in Yahoo!. This search returns one

very important result: A posting to a message board by a user named nymB from the same eMail address. This clearly attaches the nymA to the nymB.[11]

A search on Yahoo! for "nymB" returns four results, one of which is the previously mentioned post. From this posting we can determine that nymB loves the "King's Quest" series of computer games, and has loved them from an early age.

At first glance, the second result, which contains user profiles from the Web site http://www.dalantech.com, appears to be a false positive, as the eMail address for the nymB listed does not match any of the ones known for nymB or nymA. Inspection of the other user profiles on the page seems to reveal that none of the users (including nymB) have legitimate eMail addresses. All of the addresses appear to follow a similar pattern, which users a strange sounding domain name (many of them involving the word "keyboards" in the domain name). The address for the nymB listed on the page is lost3@crawling030lavenderkeyboards.net. No other relevant information is given that might help to determine whether this nymB is the nymB in question. A trace using Visual Route 7.0g to the domain http://www.crawling030lavenderkeyboards.net failed at the DNS query, which Visual Route was unable to resolve. A WHOIS lookup to the lookup server at whois.internic.net for the domain http://www.crawling030lavenderkeyboards.net using DreamSysSoft's ANT 2.7 (Advanced Net Tools) returned the result that the domain did not exits. These queries prove that this address is not a valid address for the nymB listed. After examining the addresses listed for other users, it appears that the site places fake eMail addresses in a user's profile if they do not enter a real address. Further inspection is required to determine whether the nymB listed on the site is the nymB in question.

[11] Again it must be stated that someone could be impersonating the true name behind the nyms. Stylistically, messages from nymB will fit the pattern of those created by nymA.

The user nymB has written two posts to the message boards at http://www.dalantech.com, and a link exists in the user's profile to display all of the posts written by a given user. The two posts by this nymB have some revealing traits: They are both to a thread in the networking forum created by nymB, and they are regarding the procedures for wiring Category 5 keystone jacks for placement in wall plates. It seems that the true name behind this nymB was having trouble getting the wired keystone jacks to operate properly. The style of the postings seems to match that of the nymB in question. Examination of nymA's resume (available from nymA's Web Site) shows that nymA does have experience with wiring keystone jacks and installing premise wiring. So it appears that a search result that originally seemed like a false positive has turned into a fairly certain match.

The third result from the Yahoo! search for "nymB" leads to two posts in the forums at the Concord Blue Devils drum corps site. Earlier we established that the true name behind nymA is a drum corps fan, and once had a fantasy drum corps team, so it seems that this nymB might be a match to the one in question. Clicking on the username reveals the users' profiles, and the profile for nymB reveals that it is a match, as this nymB lists an eMail address that matches one of the eMail addresses established for nymA. The other attributes listed (real name and age) also match the nymA in question. From the two posts, we can determine that nymB does not like the Blue Devils 2002 show because nymB thinks that it is boring and does not push the envelope enough.

The final result returned from the Yahoo! search is a posting on http://www.resellerratings.com regarding QbitPC.com, a computer retailer. nymB was apparently surprised by all of the negative ratings that QbitPC.com had been receiving, stating that nymB had ordered from them a number of times and was always fully satisfied.

One of the more disturbing examples of information available on Web is the phone book feature of the Google search engine. The Google search engine can return the name, address and phone number of any publicly listed phone number in the US. All that is required to find an individual's information is to type their name and state of residence into the search engine. For example, to search for the residence information of a John Doe living in California, the search would be "John Doe CA". Successful search results include links for Yahoo! Maps and Mapquest, which allow the searcher to create a map to the residence with the click of a button. Searches for nymA returned no results, signaling that nymA does not have a telephone and residence listed under nymA's true name, or the number is unlisted. In addition, Google supports "reverse phone number lookups", which use a phone number to discover the associated name and location. An example of a reverse phone number search would be "555-555-4674". If Google does not provide the requested information, there are many phone number and reverse phone number directories freely available on the Web.

By default, Google provides the contact information of every publicly listed residence US. An individual must contact Google in order to have their name removed from Google's online directory. The fact that Google chose an opt-out policy rather than an opt-in policy shows that the organization is not concerned with individual privacy.

Public Policy

The USA PATRIOT ACT: Enabling Government Monitoring

The government passed the USA PATRIOT ACT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism; Public Law 107-56) quickly after the Sept. 11, 2001 terrorist attacks to enable law enforcement to better combat terrorism. The legislation provides the government with an unprecedented ability to monitor all

aspects of the life of a citizen that is "believed to be involved in terrorism". One of the problems with the USA PATRIOT ACT is the definition of terrorism and terrorist. One only needs to remember the McCarthy Communist hearings to understand why the USA PATRIOT ACT presents a scary proposition, as the act opens the door for widespread racism and ethnic stereotyping by the government. In addition, the USA PATRIOT ACT redefined a number of crimes, including Web Site hacking, as acts of terrorism. The act defines all instances of hacking as terrorist acts and states that punishment should follow along those lines. Less vicious crimes such as Web Site defacement or executing a DoS (Denial of Service) attack could result in a lengthy prison sentence, a loss of computer privileges and possibly deportation (for foreign-born defendants). This is a terrible categorization for hacking and overextends the suppressive powers of the government. Defacing a Web Site is a minor offense when compared with terrorist attacks such as the bombing of the U.S.S. Cole or the September 11, 2001 attacks.

Although the legislation is supposed to combat terrorism, many experts question the nearly unlimited powers granted to law enforcement by the USA PATRIOT ACT. According to Debbie Howlett, "...critics say it's a threat to civil liberties. And three states – Hawaii, Alaska and Vermont – plus 134 cities and counties have approved resolutions calling for a repeal of the act..." (3A). Citizens are standing against the sweeping powers enacted by the USA PATRIOT ACT because it threatens civil liberties to the point where George Orwell's "1984" seems more fact than fiction. It gives the government unlimited access to all of an individual's panoptic information, from their grocery shopping habits to their library records. According to Howlett, "The 342-page Patriot Act was signed into law six weeks after the Sept. 11 terrorist attacks. It expands the power of the federal government to wiretap cellphones, check library records,

eavesdrop on computer use, access financial records and detain terrorism suspects without charges" (3A).

The USA PATRIOT ACT has greatly altered the way law enforcement agencies operate. According to Miller, "Under this act, authorities no longer need to obtain a court order to initiate online surveillance..." (371). In addition, law enforcement now has the ability to detain suspects indefinitely without formally filing charges against them. This provision changes the procedures of law enforcement from the traditional "innocent until proven guilty" to a more tyrannical "guilty until proven innocent". According to Caron Carlson, "One provision (Section 215) allows the FBI to demand business records, such as a subject's medical history, Internet use patterns and gun purchases, with an order from the Foreign Intelligence Surveillance Court, even if the subject is not a suspected terrorist. Critics say the order amounts to a rubber stamp" ("Rights Advocates"). The FISC (Foreign Intelligence Surveillance Court) is a court system that requires far less supporting evidence than the traditional court system for issuing a warrant. The USA PATRIOT ACT relaxed the guidelines for taking a case before the FISC. According to Carlson,

"Another provision (Section 505) gives the government greater power to use what is known as a "national security letter"—also known as an administrative subpoena—to obtain records such as credit reports, financial documents, and telephone and email bills. A national security letter does not require law enforcement to show probable cause, nor does it require even the low standard of judicial review required by a FISA Court order" ("Rights Advocates").

Outraged citizens have been protesting the USA PATRIOT ACT since its enactment. "In Berkeley, Calif., public library director Jackie Griffin purges records of all returned books each day and erases the list of Web sites visited on the library's 50 Internet terminals" (Howlett 3A).

According to Amy Goldstein,

> "In Seattle, the public library printed 3,000 bookmarks to alert patrons that the FBI could, in the name of national security, seek permission from a secret federal court to inspect their reading and computer records - and prohibit librarians from revealing that a search had taken place... And in Hillsboro, Ore., Police Chief Ron Louie has ordered his officers to refuse to assist any federal terrorism investigations that his department believes violate state law or constitutional rights".

While citizens are fighting against the USA PATRIOT ACT, select government officials are trying to strengthen its powers. "Attorney General John Ashcroft asked Congress Thursday [5 June 2003] to widen the USA Patriot Act so that suspected terrorists can be held indefinitely before trials and to let him seek the death penalty or life imprisonment for any terrorist act" (MSNBC "Ashcroft"). Providing the USG with unlimited powers of surveillance and retention is a threat to every citizen, and it did not take the administration long to exploit the new law. "The [Justice] department's inspector general found 'significant problems' in the Bush administration's actions toward 762 foreigners held on immigration violations after the [Sept. 11] attacks. Only one, Zacarias Moussaoui, has been charged in the United States with a terrorism-related crime; 505 have been deported" (MSNBC "Ashcroft").

From the first day of the legislation's enactment it was clear that the USA PATRIOT ACT might be "patriotic" in the sense that "Americans are superior", but it was definitely not constitutional. The mere idea of choosing the name "USA PATRIOT ACT" for the legislation signals that government officials knew that getting the legislation passed and supported would require more marketing savvy than political skill. By choosing to name the legislation the "USA PATRIOT ACT", the government was attempting to ride the high tide of flag-waving patriotism

that arose after September 11, 2001, while simultaneously asserting that anyone who does not support a bill named the "PATRIOT ACT" is unpatriotic.

The FBI (Federal Bureau of Investigation) has used the USA PATRIOT ACT to allow secret searches and seizures by classifying them as intelligence investigations rather than criminal investigations. By feeding off the FUD (Fear, Uncertainty and Doubt) created by the events of September 11, 2001, the FBI thought it could freely invade individuals' privacy. According to Dan Eggen,

> "To civil libertarians and many defense lawyers, the changes pose a threat to the privacy and due-process rights of civilians because they essentially eliminate...the traditional boundaries separating criminal and intelligence investigations. As a result, these critics say, FBI agents and federal prosecutors will conduct many more searches and seizures in secret, as allowed under intelligence laws, rather than being constrained by the rules of traditional criminal warrants" (A01).

Before the USA PATRIOT ACT, the FBI had to separate the intelligence-gathering portion of an investigation from the criminal investigation portion (Eggen A01). Now, the FBI can categorize an incident as a counterterrorism case from the start, allowing intelligence and criminal investigators to work together (Eggen A01). One must question who will be defining terrorism and to what extent the FBI will be willing to operate against innocent individuals for the purpose of gratuitous information gathering sessions. The FBI hopes that the new rules closing the gap between intelligence gathering and criminal investigations will allow them to prevent future terrorist events. Unfortunately, we still have yet to hear exactly how the FBI believes "terrorists" behave.

Past cases in which discord between FBI agents and criminal investigators caused a suspect to evade capture prove the necessity of restructuring. However, we must wonder how far the FBI will carry their new methods of operation. According to Eggen, "According to a study released this week [December 2003] by Syracuse University's Transactional Records Access Clearinghouse, Justice and the FBI have sharply increased the number of terrorism cases they are pursuing since the 2001 attacks, although most of the 6,400 people referred to prosecutors were never charged with a crime related to terrorism" (A01). Eggen quoted Michael A. Vatis, a former Justice Department and FBI official, as saying that the new changes were necessary but oversight was critical to assure that agents did not overreach in their investigations, which the prior structure prevented (A01). We can only hope that someone provides the necessary oversight and guidance to prevent the FBI turning the US into a quasi-police state.

Unfortunately, we must consider the worst-case scenario, as the FBI has a long history of abusing its power that continues today. According to an AP (Associated Press) report,

> "The Federal Bureau of Investigation has been collecting information on the tactics, training and organization of antiwar demonstrators, The New York Times reported in Sunday editions...The memo analyzed legal activities such as recruiting demonstrators, as well as illegal ones such as using false documentation to gain access to secured sites..." (MSNBC "FBI collecting").

The FBI claims that monitoring is necessary to prevent anarchists and terrorist groups from committing violent acts, yet they are inadvertently (or intentionally) monitoring both threatening and non-threatening activities, and invading the basic right to free speech. Repeated abuses by the FBI during the 1960s and 1970s (including spying on Dr. Martin Luther King, Jr.) led to many of the rules that have restricted the FBI's operations for the past two decades (MSNBC

"FBI collecting"). Attorney General John Ashcroft relaxed most of those rules after September 11, 2001.

Fortunately, the ACLU (American Civil Liberties Union), EPIC, EFF (Electronic Frontier Foundation) and others will not accept the USG's trampling of individual rights.

> "The American Civil Liberties Union is challenging the FBI's use of expanded powers to compel Internet service providers to turn over information about their customers or subscribers...The FBI can issue national security letters, or NSLs, without a judge's approval in terrorism and espionage cases. They require telephone companies, Internet service providers, banks, credit bureaus and other businesses to produce highly personal records about their customers or subscribers" (MSNBC "ACLU battles").

According to MSNBC,

> "The lawsuit challenges as unconstitutional one of several types of national security letters used by the FBI in counterintelligence and counterterrorism investigations. The letters in question involve records held by Internet service providers about their clients, including billing information, kinds of merchandise the clients buy online and the e-mail addresses of the clients' associates" ("ACLU battles").

The FBI is gathering data in secret, without a warrant and the Bureau does not disclose what happens to the data once it is gathered. The FBI could be adding the information it gathers to its existing data collection and enhancing its knowledge regarding every citizen in the US. In fact, because of the USA PATRIOT ACT, the FBI can monitor someone without due cause, and does not need to prove any justification regarding why they are monitoring an individual to the individual or the organization from which they are gathering information (MSNBC "ACLU battles").

Most actions performed under the USA PATRIOT ACT have been under veiled secrecy to protect them from the opinion of the American public. The veil of secrecy has only intensified feelings regarding the USA PATRIOT ACT, and resistance to the legislation has been so fierce that Attorney General John Ashcroft and President George W. Bush have been separately touring the nation in an attempt to rally support for the law. At every stop, they are met with applause from the people listening to their respective speeches (mostly law enforcement officials), while outside protesters demonstrate in outrage. As the election draws near, each is stepping up their campaign to gain support for the USA PATRIOT ACT's renewal. There is hope in the signs of dwindling support in Congress. According to the AP, "Several conservative Republicans have joined liberal Democrats in saying that portions of the law are too intrusive on Americans' lives. They are threatening to allow the provisions to die at the end of next year. Some want to impose more judicial oversight of how police and prosecutors conduct investigations" (MSNBC "Bush urges"). In 2004, Ashcroft released some statistics on PATRIOT ACT usage in an attempt to convince Congress not to weaken the law when it comes up for renewal in 2005. An AP story covering Ashcroft's announcement stated that "Powers permitted under the Patriot Act have also been used in investigations involving potential school bomb attacks, computer hackers, child pornography, violent fugitives and illegal weapons sales" ("Ashcroft details"). Defining child pornography and hacking as terrorism is an interesting way of deflecting criticism that law enforcement officials are overreaching with the powers given to them by the PATRIOT ACT, but it fits with the government's recent practices. One subject that Ashcroft's report did not detail was whether law enforcement officials had seized library or video rental records, which they were not able to do before the PATRIOT ACT. According to the AP report, "The report did not say whether the FBI had used its authority to obtain library or bookstore records. That

information is classified, but Ashcroft last year issued a declassified statement saying that, up to that point, the power had not been used" ("Ashcroft details"). A Congressional vote one week prior to the release of Ashcroft's report narrowly upheld the ability to search library records. The mere fact that top ranking US officials feel that it is necessary to trumpet the law's benefits years before its renewal is a sign that they question its perception and future.

The fight against the PATRIOT ACT is still underway, with victories slowly mounting for those challenging the act. On June 15, 2005, the US House of Representatives voted to disallow investigators to examine library records or bookstore sales receipts. This vote presents an opening for Congress to repeal additional powers granted under the PATRIOT ACT during the act's sunset period.

Collecting the data

A number of countries are participating in extensive information gathering. According to a story reported by the AP in April 2003, "Over the past 18 months, the U.S. government has bought access to data on hundreds of millions of residents of 10 Latin American countries — apparently without their consent or knowledge — allowing myriad federal agencies to track foreigners entering and living in the United States" (MSNBC "U.S. buys"). Despite claims to the contrary, the USG is currently involved in practices that undermine the basic privacy rights of individuals worldwide.

Citizens of Latin American countries pose no threat to US citizens, yet the USG feels that it is necessary to purchase the personal information of hundreds of millions of Latin Americans. This privacy invasion does not involve citizens from certain Middle Eastern nations proven to have committed terrorist acts against the US. This is an intrusion against the people of Latin America, who at worst sneak across the US border and saturate the job and welfare markets.

Even so, illegal immigration generally tends to involve a few individuals from a few select countries, and not anywhere near one million people, much less hundreds of millions of people.

The same article also states, "The practice broadens a trend that has an information-hungry U.S. government increasingly buying personal data on Americans and foreigners alike from commercial vendors including ChoicePoint and LexisNexis" (MSNBC "U.S. buys"). According to Carlson,

> "Fighting terrorism on the home front has given the U.S. government a big appetite for information, with records such as credit reports, charity lists and traffic incidents being scoured for leads in the name of national security. This zeal to cross-check and profile citizens is creating a rush of companies eager to sell the fruits of private and public databases to federal agencies" ("Who's Minding").

The USG is buying and warehousing data on all foreigners and Americans, regardless of those individuals' criminal or social background. The USG has repeatedly claimed that the data warehousing and data mining techniques in question comprise a multi-faceted anti-terrorism system, aimed at making the country safer from terrorist threats. Assuming that is a true statement (which further analysis will soundly disprove), each individual must question to what extend they are willing to sacrifice individual privacy and leisure to prevent terrorism. Given previous operations of the USG, believing that warehousing and mining of data is truly only for anti-terrorism preventions is a monumental mistake.[12] These events show that the USG is never concerned only with foreigners and suspected terrorists, but with every citizen of the world.

Regarding the information purchased on Latin American citizens, the data gathered includes phone numbers (listed and unlisted), addresses, passport numbers and driving records, originally received from organizations that register voters or issue national IDs or driver's

[12] The McCarthy Communist Trials stand as a prime example of "information" misuse.

licenses (MSNBC "U.S. buys"). According to the article, the approximately 31 million residents of Colombia have the most fear: "In Colombia, ChoicePoint buys the entire country's citizen ID database, including each resident's date and place of birth, passport and national ID number, parentage and physical description" (MSNBC "U.S. buys"). The situation threatening Colombian citizens begins with the country itself: No country should have such a comprehensive database of its citizens (although later we will discover that the USG is trying to develop a database of US citizens). National database systems are a threat to privacy and humanity. Someone should first convince the government of Colombia to destroy its database. That the USG would support the actions of the Colombian government by purchasing the entire database only shows how invasive our government is willing to become in its quest for data.

Worse, it appears that the government does not care about the accuracy of the data gathered, or its origin. According to Carlson,

> "Thus far, the government appears unconcerned about regulating its sources of personal data. The FBI's use of commercial databases has grown 9,600 percent over the last decade, according to EPIC. The bureau uses credit records, property records, professional licenses, driver's licenses and other data purchased from companies such as ChoicePoint Inc., of Alpharetta, Ga., and LexisNexis, of Dayton, Ohio, as well as credit reporting agencies such as Atlanta-based Equifax Inc., Experian Information Solutions Inc., of Costa Mesa, Calif., and Trans Union LLC, of Chicago. But none of these companies is held accountable for the truth or accuracy of the information it sells" ("Who's Minding").

According to Sullivan, ChoicePoints records on a given consumer, sometimes 20 pages or longer, are often riddled with errors ("ChoicePoint files"). Sullivan continues to recount the story

of Deborah Pierce, a privacy advocate who managed to obtain a copy of her information from ChoicePoint. According to Sullivan,

> "A dozen former addresses were listed, along with neighbors and their phone numbers. Almost 20 people were listed as relatives -- and their neighbors were listed, too. There were cars she supposedly owned, businesses she supposedly worked for. But the more closely she looked, the more alarmed she became: The report was littered with mistakes" ("ChoicePoint files").

Sullivan continues,

> "Under former addresses, an ex-boyfriend's address was listed. Pierce said she never lived there, and in fact, he moved into that house after they broke up. The report also listed three automobiles she never owned and three companies listed that she never owned or worked for. Under the relatives section, her sister's ex-husband was listed. And there are seven other people listed as relatives who Pierce doesn't know" ("ChoicePoint files").

Richard Smith, another privacy advocate, also purchased his information from ChoicePoint. According to Sullivan, "Some of the mistakes on Smith's report were comical: That his wife had a child three years before they were married, that he had been married previously to another woman, and most absurd, that he had died in 1976" ("ChoicePoint files"). Of course, ChoicePoint does not provide consumers with any way to correct their personal information in the company's files, leaving consumers to worry that mistakes on someone else's part could cost them employment, a loan, or cause legal trouble. The cross-purpose use of data is also questionable. According to Carlson,

"The question of how data is used by the government is at the center of privacy and database security concerns. Evolving data mining technologies create new ways to manipulate, share and apply data, enabling information gathered for one purpose to be used for another" ("Who's Minding"). In some countries, reusing data collected for one purpose for another dissimilar purpose is illegal. In post-September 11, 2001 US, it is not.

The uncontrolled sale of data submits the data to inaccuracies and makes it easier for the data to end up in places far from where it started. In July 2003, privacy experts discovered that Batteries.com committed multiple violations of its own privacy policy as well as of TRUSTe's membership requirements (whom certified Batteries.com's policy). Columnist David Berlind, who had purchased batteries from Batteries.com, had his information placed in the Men's Journal subscription database without his approval (Berlind "TRUSTe issues"). A further investigation found that Batteries.com shared information with a third party (a violation of its privacy policy) and shared the information without informing TRUSTe or Batteries.com customers (a violation of its TRUSTe certification) (Berlind "TRUSTe issues"). The biggest problem with this scenario is that one accidental sale to a company that does not respect privacy could cause a widespread disbursement of consumers' personal information. Consider the following scenario: An organization with a privacy policy stating that it will not sell customer data to third parties sells its customer data to a single third party entity, either on purpose or by accident. That is a violation of the organization's privacy policy. If the privacy policy of the company that purchased the data allows that organization to resell the data to additional third parties, then it can resell the data as much as it desires without causing an infraction against its own privacy policy. One mistake can cause an uninhibited spread of individuals' personal information. Unfortunately, the growth of "information brokers" has been uncontrolled, and in

late 2004 and 2005 privacy advocates worst fears came true: Multiple instances of data theft occurred at ChoicePoint and LexisNexis.

These incidents revealed the dangers of becoming a database nation, because the information was gained not through cracking or other electronic means, but through social engineering and finding weaknesses in the companies' business processes. In the case of ChoicePoint, criminals posed as legitimate companies by opening 50 new accounts with the company and received consumer data through normal transactions with ChoicePoint (Sullivan "Database giant"). According to an AP report, "In this case, the thieves — posing as check-cashing companies or debt collection firms — provided business licenses that appeared to be legitimate and used the names of real people with clean criminal records. The company caught on later by tracking the pattern of the searches conducted by the suspects" ("ChoicePoint to rescreen").

The criminals then used the data they purchased to commit crimes involving massive identity theft. The stolen information included names, addresses, SSNs, and credit reports, among other information (Sullivan "Database giant"). Although ChoicePoint originally notified only 30,000 to 35,000 consumers, the company eventually notified 145,000 nationwide, and the final total could be much higher. According to Sullivan, "The Atlanta-based company says it has 10 billion records on individuals and businesses, and sells data to 40 percent of the nation's top 1,000 companies. It also has contracts with 35 government agencies, including several law enforcement agencies" ("Database giant"). ChoicePoint does an exceptional amount of business with the information that it has collected, with revenues of $900 million annually. In part, due to fears of retaliation from the Attorney Generals of 38 states, and threats of contract cancellations, ChoicePoint sent the notification letters, and has offered to pay for credit monitoring services for

one year for all of the potential victims (AP "ChoicePoint to rescreen"). The latest reporting had uncovered 750 people who actually suffered identity theft resulting from the ChoicePoint compromise (AP "ChoicePoint to rescreen").

In the case of LexisNexis, thieves accessed the company's databases through electronic intrusion. According to an AP Report, "Using stolen passwords from legitimate customers, intruders accessed personal information on as many as 32,000 U.S. citizens in a database owned by the information broker LexisNexis, the company said" ("Another big"). This is startling and disturbing, because not only does one have to worry about the large information brokers, but they also have to worry about the security practices and business processes of all of the companies that execute transactions with information brokers. A customer's poor security practices could spell disaster for their partners. The most startling fact might be the value LexisNexis gives to consumers' information. According to the AP report, "The database that was compromised, called Accurint, sells reports for $4.50 each that include an individual's Social Security number, past addresses, date of birth and voter registration information, including party affiliation" ("Another big"). It is an interesting point to note that the database is maintained by the Seisint unit of LexisNexis, which the company purchased in August (AP "Another big"). Seisint was previously know as the company behind the controversial Matrix law enforcement database project, originally funded by a number of states, all of whom eventually withdrew from the project, citing security and privacy concerns (AP "Another big").

One can only hope that ChoicePoint and LexisNexis will notify all effected customers, and greatly improve their processes. As it stands, both companies could be in risk of violations of current legislations because of the failure of their internal processes. One does have to wonder

though, if potential foreign victims have been notified of the breaches. It stands to reason that most, if not all of the victims were from the US, but what if they were not?

TIA: The Government's Data Warehouse

The pinnacle of the government's privacy invasions is the TIA (Total Information Awareness) system. The government seeks to store all of the panoptic information describing an individual in a massive data warehouse, including images of their face, video of their gait, financial information, personal information, shopping information, medical information and professional information. With all of this information at their disposal, the government could easily monitor and track residents of the US. The government plans to use advanced data mining techniques to develop correlations between individuals and their activities. The original logo for the IAO (Information Awareness Office), which oversees the TIA system and related programs, adequately justifies the fear generated by the project:

If a giant eyeball casting a gaze over the surface of the planet is not scary enough, then consider that the Latin text at the bottom ("SCIENTIA EST POTENTIA") translates to "Knowledge is power". Shortly after the logo made its debut, the IAO removed it from their Web site, along

with the biographies of the officials in charge of the TIA project. The IAO then proceeded to rename the TIA system as "Terrorist Information System", hoping to generate support from US citizens' post-September 11, 2001 terrorist fears.

The initiatives under development as part of the TIA program cover all aspects of privacy invasion. For example, researcher Teresa Lunt is developing a privacy appliance under the Project Genisys branch on the TIA program (Fordahl 5E). The device would give the owner of a data warehouse control over data sharing specifics in response to a request for data. When the device receives a request for information fitting a set of criteria, it returns the records for all of the individuals in the warehouse that meet the criteria, but not before filtering out any personally identifying information. Investigators could use subsequent queries to narrow down the number of individuals in the pool to a smaller number, at which point they would be required to secure a warrant before receiving the individuals' identification. As with most technological innovations, there are positive and negative aspects to the privacy appliance. According to David Sobel, "What is the standard the judge is going to be judging this on? We're talking about someone who might have a proclivity to commit a crime that has not yet been committed. This is just something that is completely alien to our judicial system" (qtd. in Fordhal 5E). Without proper oversight and auditing, there is no way to stop an investigative agency from manipulating queries to obtain the results they desire. Investigators could easily construct a set of queries to return all male, Islamic, Middle Eastern individuals that are flying on an airline in the next month, convince a judge that they are suspected as part of some fabricated plot, and imprison them indefinitely.

Even the device's designer does not understand its full potential. According to Fordahl,

> "She [Lunt] admits that she is not fully aware of all the government's plans. But as she understands it, government analysts won't be fishing through data swept into a central database. Rather, they will first create models of suspicious activities, and then query privately controlled databases protected by privacy appliances to find out numbers-but not identities-of people matching certain traits" (5E).

Lunt completely misunderstands the situation on a number of points. First, the article previously stated that law enforcement officials could gain permission to identify individuals by obtaining a warrant from a judge. After all, it would not have been very useful to know before the Sept. 11, 2001 WTC tragedies that an unknown number of unidentified individuals might be planning a terrorist attack. Second, having access to multiple private databases is the same as having access to one centralized database. Manually performing queries to multiple tables in multiple databases is analogous to performing a SEQUEL join on the tables or having all of the information in one database. This is the basic definition of the panoptic sort. Third, there is no one to provide oversight of the operations or control data management. We know that the government desires to create one large centralized database containing the panoptic information describing every resident of the US. There is no one to prevent law enforcement officials from reusing the data regarding a group of potential suspects in their own centralized database. Once law enforcement officials obtain a warrant to identify the potential suspects, they could hand the data over to the DoD for entry into the main TIA database. Regardless, the development of the privacy appliance proves that the USG plans to execute a panoptic sort on "suspected terrorists". It is frightening to consider that the USG possesses these capabilities.

These facts raise additional questions regarding the two previously mentioned persistent digital nym platforms. The government may decide against maintaining a large centralized data

warehouse, if they can rely on Microsoft and the Liberty Alliance to maintain a database for them. According to Larry Diffey, "This, of course, makes it that much easier for the government, under the guise of the Patriot Act, to procure this information. What would prevent the government from keeping constant tabs on all Passport usage in the interest of national security?" (40).

In an attempt to display their dismay at the government's new operations, individual citizens and citizen groups have bought and displayed the personal information of selected government officials. According to Jennifer C. Kerr, "The California-based Foundation for Taxpayer and Consumer Rights said for $26 each it was able to purchase the Social Security numbers and home addresses for Tenet, Ashcroft, and other top Bush administration officials, including Karl Rove, the president's chief political advisor" ("Privacy advocates"). The specific reason for this action (beyond proving the insecurity of personal information) was to protest House legislation intended on protecting consumer rights. According to Kerr, "While backing the overall goals of the bill, the group's executive director, Jamie Court, objected to a portion of it that would continue a current pre-emption of tougher state privacy laws" ("Privacy advocates"). The group's main concern was that the law did not regulate large conglomerate corporations that fail to monitor their inter-organizational information sharing. According to Kerr, "For example, a banking corporation might have a number of insurance, securities and real estate affiliates it does business with and financial data might be swapped among all" ("Privacy advocates").

Other attacks on the TIA system have directly targeted Admiral John Poindexter (Ret.), after a suggestion in Matt Smith's column for "sfweekly.com" that the government should learn first-hand the dangers of the TIA system. In his article, Smith published personal information regarding Poindexter, including his home phone number, address, wife's name and information

about her religious convictions. There was an instant response to Smith's column: The "cryptome eyeball series" (http://cryptome.org/eyeball.htm) contains high-resolution satellite photos of US government and military installations. The "Eyeballing Total Information Awareness" page (http://cryptome.org/tia-eyeball.htm) provides Poindexter's name, address, telephone number, satellite photos of his house and directions to his house. Another Web site (http://fyre.sytes.net:8007/pictures.html) contains pictures of Poindexter's house taken from the street out-front. This information resulted in the Poindexters' receiving an unrelenting stream of telephone calls to their residence, complaining about the TIA system.

On July 17, 2003, the US Senate voted unanimously to cut funding for the TIA system. The final Congressional budget officially terminated the TIA system, and appears to have disbanded the IAO (the Office's Web site no longer exists). Given the overly secretive history of the USG, it is imperative that privacy organizations continue to pay close attention to the government's actions. The government has already shown it willingness to monitor citizens with the Carnivore system.[13] The Area 51 research facility has long been a secret among secrets, proven to exist only through satellite photos and warning signs that dot its far perimeter. Some secrets, such as the (formerly) secret underground city at Green Briar, are necessary for our

[13] The Carnivore program is part of a suite of programs known as the "DragonWare Suite". The FBI utilizes the DragonWare suite to track "suspected criminals". This suite of programs captures packets, reassembles them, and facilitates data mining operations on the recovered data. FBI agents install a computer with the DragonWare Suite at an ISP, and begin capturing data. One problem with the system is that the FBI has not yet developed a way for it to capture only data relating to the suspected criminal. In fact, this seems to be an interesting wordplay on the name "Carnivore". A carnivorous dinosaur eats any type of meat without being selective or choosy. The Carnivore portion of the suite captures and analyzes all traffic from all users without being selective or choosy. Other fears include corrupt officials who use the DragonWare Suite to spy on innocent individuals. Compounding the problems is that under the USA PATRIOT ACT the FBI no longer has to obtain a warrant to use the DragonWare Suite. Some ISPs, including AOL (America Online) and Earthlink, have publicly refused to allow the FBI to bring a computer with DragonWare Suite installed into their facilities, even with a court order. In the end, the FBI used Carnivore only 25 times, between 1998 and 2000 (AP "FBI abandons"). The total cost of the failed Carnivore project was between $6 million and $15 million (AP "FBI abandons"). On January 18, 2005, the FBI announced that it was canceling the project in favor of using commercial software instead (AP "FBI abandons").

national safety. However, we must continually strive to uncover secrets that threaten the privacy, sanity, or basic human condition of the country's residents.

Ultimately, the status of programs such as the TIA may prove irrelevant, as we come closer to realizing the fullest potential of the NII. In the TIA program the government desired a centralized location to gather, store, and mine individuals' panoptic information. Even without a centralized data store, as the NII develops and the information about each human being stored at various locations grows, the government will still be able to access all of the information using a panoptic sort.

Other Programs

It appears that the fight for information privacy may never end, as the end of one program only signals the start of another. Congress may have stopped the TIA system, but that was a federal program. State-level programs do not fall under the direct influence of Congress, unless a law specifically prohibits any form of a program at any level, and state-level programs are appearing that are every bit as dangerous as the TIA system. According to Robert O'Harrow Jr.,

> "Police in Florida are creating a counterterrorism database designed to give law enforcement agencies around the country a powerful new tool to analyze billions of records about both criminal and ordinary Americans. Organizers said the system, dubbed Matrix, enables investigators to find patterns and links among people and events faster than ever before, combining police records with commercially available collections of personal information about most American adults. It would let authorities, for instance, instantly find the name and address of every brown-haired owner of a red Ford pickup truck in a 20-mile radius of a suspicious event" ("U.S. Backs").

According to O'Harrow Jr., "The Justice Department has provided $4 million to expand the Matrix program nationally and will provide the computer network for information sharing among the states...At least a dozen states – including Pennsylvania, New York, and Michigan – said they want to add their records ("U.S. Backs"). Even those connected to the project fear its power. According to O'Harrow Jr., "A senior official acknowledged it could be intrusive and pledged to use it with restraint. 'It's scary. It could be abused. I mean, I can call up everything about you, your pictures and pictures of your neighbors,' said Phil Ramer, special agent in charge of statewide intelligence. 'Our biggest problem now is that everybody who hears about it wants it' " ("U.S. Backs").

Government Information in Public View

While attempting to gather all of the US residents' panoptic information, the USG has failed to secure its own information, as illustrated by Sean Gorman, a graduate student at GMU (George Mason University). Gorman created a computerized map of the US, detailing its entire fiber optic infrastructure (Laura Blumenfeld "Dissertation could"). According to Blumenfeld,

> "He can click on a bank in Manhattan and see who has communication lines running into it and where. He can zoom in on Baltimore and find the choke point for trucking warehouses. He can drill into a cable trench between Kansas and Colorado and determine how to create the most havoc with a hedge clipper" ("Dissertation could").

Gorman's project, like many other research projects in the post-September 11, 2001 world, is coming under scrutiny from the government and law enforcement officials for the threat that it poses to national security. As with standard government operating procedures, they treat Gorman as the criminal, even though he gathered all of the information for his project from public sources, in print and on the Internet.

Gorman's project did not interest anyone until after the September 11, 2001 terrorist attacks. Officials then realized that his project had created an interactive map that terrorists could use to cripple the nation's critical infrastructure. According to Blumenfeld, "Every fiber, thin an a hair, carries the impulses responsible for Internet traffic, telephones, cell phones, military communications, bank transfers, air traffic control, signals to the power grids and water systems, among other things" ("Dissertation could"). At one end of the spectrum, a split in a fiber optic line could render a city without Internet access for days, a situation this thesis' author experienced first-hand. At the other end of the spectrum, a split to the correct fiber backbone could render an entire region without electricity, water or other critical resources.

Gorman and his research partner now work on their project under strict security guidelines imposed by GMU. According to Blumenfeld, "...[the project is] sitting in a gray cinderblock lab secured by an electronic lock, multiple sign-on codes, and a paper shredder...When their computer crashed, they removed the hard drive, froze it, smashed it and rubbed magnets over the surface to erase the data" ("Dissertation could"). Imposing these strict security guidelines may have been the only way for GMU to allow the project to continue, given the intense pressure from businesses and the government for them to terminate and destroy the project. Unfortunately, the government chose to intimidate an innocent student, rather than focus on removing potentially dangerous information from publicly available resources.

Cameras on Every Corner

In modern society, we should assume that we cannot escape Big Brother's gaze, because that appears to be the unfortunate truth. Consider the case of David Horton, whom police arrested at a Cincinnati Reds professional baseball game, after his face appeared in a crowd shot on the 'Kiss Cam' (MSNBC "Wanted man"). Coincidentally, his parole officer was also at the

game, and recognized Horton on the video screen (MSNBC "Wanted man"). Department stores have long used cameras hidden in the eyes of mannequins as video surveillance to catch shoplifters. In this case, security is only concerned with preventing shoplifting. What happens when the government decides to watch everyone? What happens when the goal is not to watch for specific actions, but to watch and record all actions, as is the goal of the HumanID (Human Identification at a Distance) program?

The IAO originall developed the HumanID program as part of the TIA program. According to the IAO's Web site (no longer available on the Web), the goal of the HumanID program is to:

> "...develop automated biometric identification technologies to detect, recognize and identify humans at great distances. These technologies will provide critical early warning support for force protection and homeland defense against terrorist, criminal, and other human-based threats, and will prevent or decrease the success rate of such attacks against DoD operational facilities and installations. Methods for fusing biometric technologies into advanced human identification systems will be developed to enable faster, more accurate and unconstrained identification of humans at significant standoff distances".

In short, the goal of the program is to be able to recognize any human being from a distance of 500 feet away, using their facial features, retinal scans and gait characteristics as identifiers. In order for this technology to work, the government must have access to information regarding an individual's facial, retinal and gait patterns, which adds to the evidence supporting the government's desire to create one central database as part of the now-defunct TIA program. According to the former IAO Web site, one of the plans for the system in the 2004 calendar year is to "Fuse face and gait recognition into a 24/7 human identification system". The evidence is

astoundingly clear that the government plans to monitor every individual in this country to "prevent crime", or more likely, to control society.

In order for the HumanID program to be effective, the government must place networked cameras in public places. The cameras would send face scans of individuals to a computer that can analyze and display them for a human investigator. The government could require stores that use hidden cameras to provide them with access to the video, so that they might add it to their data warehouse.

The government secretly tested facial recognition systems during the 2001 Super Bowl in Tampa Bay, Florida. Hidden cameras secretly scanned the face of every individual that entered the stadium that day, in an attempt to determine if they posed a threat to security (Robert Trigaux "Cameras scanned"). According to Trigaux, "In milliseconds, each facial image was digitized and checked electronically against computer files of known criminals, terrorists and con artists of the Tampa Police Department, the FBI and other state and local law enforcement agencies" ("Cameras scanned"). The experiment was only mildly successful. "It turns out that facial-scan technology works best when it's used to confirm whether people are who they say they are. Picking a crook out of a cast of thousands is a lot harder, and false alarms are more common" (Randy Dotinga "Biometrics Benched"). False alarms are not desirable when the question revolves around possibly detaining an individual, and the system must be highly accurate and reliable. There were some successes though, "Afterward Tampa Bay police reported that the technology pinpointed 19 people with criminal records out of a crowd of 100,000" (Dotinga "Biometrics Benched"). Notice that the system found individuals with criminal records, not necessarily individuals wanted for questioning or that posed a potential threat. Since law enforcement chose not to detain any of those individuals, their record must not have seemed

threatening. This leads us to the problems of jumping to conclusions and allowing individuals to overcome their past mstakes. Many people have criminal records, often for things done carelessly in their younger years. People make mistakes, and it is important to be able to put those mistakes in the past and move on. Perhaps the officer viewing the biometric scans and personal data is the individual's neighbor, and did not know about his neighbor's past errors. Now something that should be private and confidential has the opportunity to spread through gossip.

Another place where cameras have become prevalent is retail stores. For a short time, the emphasis on placing cameras in a store was to hide them from a potential shoplifter's view. Hidden cameras that caught shoplifters required stores to spend time and resources dealing with the prosecution of the shoplifters. For this reason, the emphasis has switched to cameras that are in plain sight. Many stores place signs near the store entrance, warning of camera usage. This strategy greatly deters shoplifting attempts and saves money for the stores. This approach might seem ideal, because the warning sign allows a potential shopper to decide if they want to shop in a store that films innocent shoppers. Not only are shoppers recorded, but in many stores they are recorded everywhere they wander.

If the paranoia over the presence of cameras seems unfounded, then one only needs to examine Britain, where cameras record the public on a daily basis. According to Jane Black, "Britain has 4,500 speed cams. The country's more than 2.5 million CCTV [closed-circuit television] cameras catch each British resident as many as 300 times each day" ("Smile, you're"). The cameras, used to catch speeding motorists and record minor traffic violations, have angered British citizens to the point where vandalism aimed at destroying the cameras occurs weekly (Black "Smile, you're"). The delicate balance between law enforcement and obtrusive

monitoring falls out of consideration when the law enforcement method does not work. According to Black,

> "And yet, very little evidence shows that speed cams reduce road deaths or that CCTV deters crime...Instead, there's an overwhelming feeling that too often surveillance is used not to make the country safer but to monitor innocent people and, in the case of speed cams, raise much-needed tax revenues" ("Smile, you're").

Statistics support the notion that the cameras only increase revenue without saving lives or preventing crimes that are more serious. According to Black,

> "From 1995 to 2001 (the latest figure available), the number of speed-cam tickets and prosecutions in Britain soared from around 207,000 to more than 1 million, while road deaths increased 4.5 percent, from 2,995 to 3,127...it's clear CCTV has done little to clean up the streets. Study after study shows that CCTV simply displaces crime to areas where no cameras are present rather than preventing it. According to a June, 2002, report from crime-fighting nonprofit NACRO, CCTV cuts crime only by 5%, vs. 20% reduction achieved by brighter street lighting" ("Smile, you're").

The study revealed a shocking truth: Rather than spending tax dollar buying cameras and spying on residents, the government could have reduced crime by installing a few more street lamps.

As with the USG, the British government could not stop with simply monitoring traffic violations. According to Black,

> "Then, on Feb. 8 — just a month after its introduction — London newspaper The Observer revealed that the system was organized in cooperation with the intelligence services, which were using facial-recognition technology to monitor individual drivers.

Suspicious motorists would be monitored not just at the point of entry but around the city" ("Smile, you're").

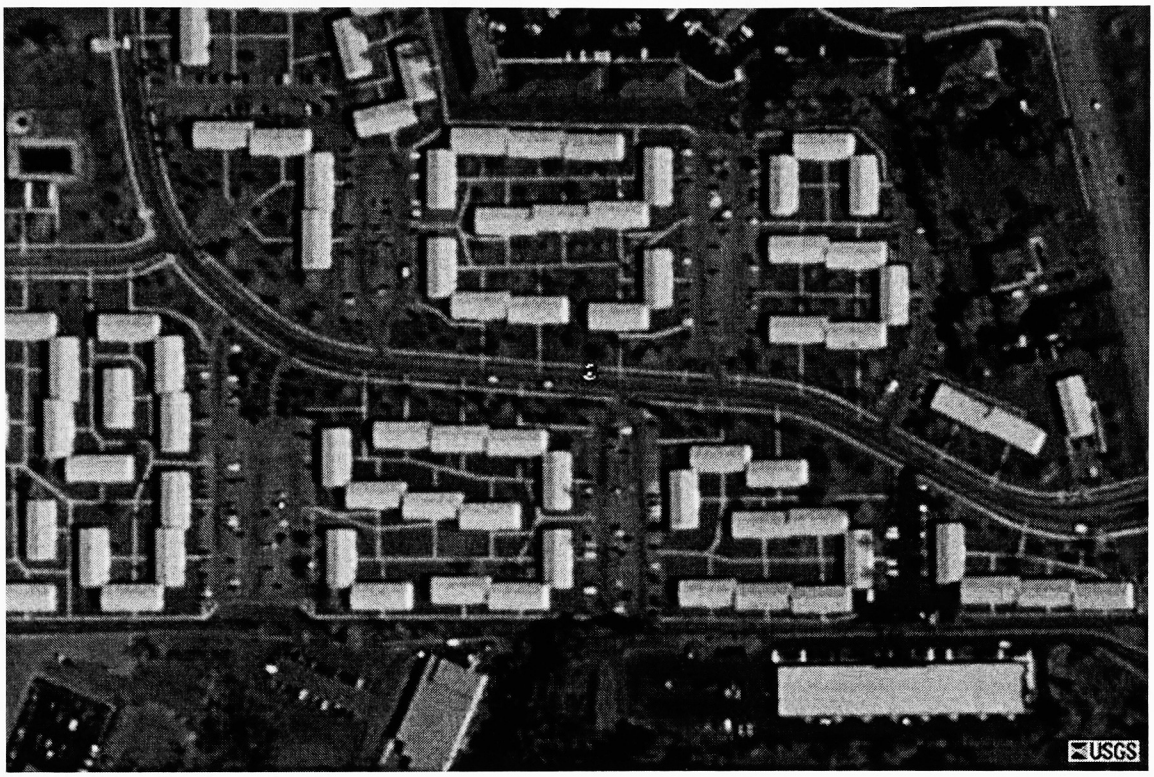
Monitoring devices could also start turning up in the most unlikely of places, as proven by a recent CIA exhibit chronicling the organization's history. According to the Reuters story, "The CIA once built a mechanical dragonfly to carry a listening device but found small gusts of wind knocked it off course so it was never used in a spy operation. The Agency also tested a 24-inch-long rubber robot catfish named "Charlie" capable of swimming inconspicuously among other fish and whose mission remains secret" ("CIA displays"). It is important to note that when the CIA developed the dragonfly in the 1970's, the organization at that time possessed the capabilities to create a miniature listening device and flying machine. One can only guess at how much the CIA might have developed and advanced its technology since then. Given the size of miniature spy cameras available from retail "spy stores", it is probably safe to assume that today the CIA can mount a camera on a mechanical dragonfly without worrying about gusts of wind. Even today's consumer recording devices excel at recording localized conversations. Modern digital voice recorders available for purchase are as small as 4 inches long, 1 inch wide and ½ an inch deep, and make excellent recordings, even when hidden under clothing.

In response to the growing number of surveillance cameras in Washington D.C., EPIC has lunched its "Observing Surveillance" campaign (http://www.observingsurveillance.org./), aimed at raising citizens' awareness of government spy cameras. The purpose of the Observing Surveillance program is to cut through the rhetoric and let the evidence speak for itself: Individuals photograph cameras around Washington D.C. (District of Columbia), and provide EPIC with the photograph along with a description of the camera's location. Only through cataloging the extent to which cameras are used can we begin to

stand against them. EPIC maintains a large repository of information regarding worldwide surveillance at http://www.epic.org/privacy/surveillance/. Amazingly, law enforcement erected the cameras in Washington D.C. without a supporting policy to govern their usage (Matha Teichner "Close Watch"). Washington D.C. is not the only place where cameras are prevalent. According to Teichner, "Every Sunday, Bill Brown conducts walking tours of the surveillance cameras in Times Square -- as many as 200 of them, by his count, out of the 5,000 he has mapped in New York City as a whole" ("Close Watch"). EarthCam (http://www.earthcam.com), a Web site that provides linkups to cameras in various locations around the world, provides a small glimpse at how many cameras are in operation worldwide (Teichner "Close Watch"). Using EarthCam you can look through cameras around the world. Remember that EarthCam shows only a small fraction of the cameras that are in existence and photographing unaware citizens.

Law enforcement officials would have us believe that they do not possess the advanced capabilities necessary to perform accurate facial recognition and track individuals walking the streets. This is not true, and an inexpensive camera purchased from any technology store has these capabilities. Worse, satellite imagery is advancing at startling rates. In 1959, the US launched the Corona satellites, which had a resolution of 5 feet (Garfinkel 96). From space, the satellites could view any object on earth that was at lease 5 feet across. In 1996, Space Imaging launched a satellite with a resolution of 1 meter, or approximately 3 feet (Garfinkel 100). Many experts believe that current spy satellites can resolve the text on the side of a cigarette package. Even non-intelligence satellites provide advanced viewing capabilities. The following photograph is of a street in Rochester, New York, taken by the USGS (United States

Geographical Survey) on April 22, 1994, and retrieved on April 30, 2004 from TerraServer USA (http://terraserver.microsoft.com):



In 1994, one decade ago, the details of streets and buildings are clear. The following image, taken on July 26, 2000, and retrieved from GeoXplorer Image Atlas (http://www.globexplorer.com/) on April 30, 2004 shows how far satellite imaging has progressed:

This image clearly displays cars, parking spaces, sidewalks and other objects in color to an amazing level of detail. The capability of modern satellites is startling and slightly unnerving. According to Garfinkel, "Whether you are on top of Mount Everest, floating on a raft in the middle of the Pacific, burying the victims of a massacre, or simply building an unauthorized pool in your backyard, today you can be absolutely alone and yet have the eyes of the world upon you" (104). Adding to the threat is the revelation that Google, a leader in technological revolutions, plans to create its own free mapping service, greatly increasing the availability and quality of satellite photographs.

The US is not the only country with questionable satellite practices. According to the Yahoo! India News coverage of a story reported by Reuters, "China plans to launch more than 100 satellites before 2020 to watch every corner of the country, state-run China Central Television quoted a government official as saying on Tuesday" ("China plans"). Officials stated that the satellites would monitor events occurring in nature and map the country's geography, as well as monitoring the activities of society, although officials would not elaborate further on the

last point (Reuters "China plans"). At least the Chinese government made its plans somewhat public. According to Dana Priest,

> "The United States is building a new generation of spy satellites designed to orbit undetected, in a highly classified program that has provoked opposition in closed congressional sessions where lawmakers have questioned its necessity and rapidly escalating price, according to U.S. officials" (A01).

Although no legislator publicly admitted that the program exists, information about it has become public as a result of the intensity of the debates taking place behind closed doors, most of which centers around the program's price tag that is skyrocketing towards $9 billion dollars (Priest A01).

NASA's Mind Reading Experiments: Pre-crime in the Physical World

As mentioned in the introduction, Orwell's novel "1984" introduced the world to the "Thought Police", who could read minds and determine if an individual was thinking any thoughts that were contrary to the beliefs espoused by Big Brother. In "Minority Report", the Pre-Crime division of the police force utilizes the abilities of three special humans to predict the future to prevent crimes before they happen. These may seem like outrageous concepts, but some government officials believe they are worth a second look. In August 2002, it was revealed that NASA (National Aeronautics and Space Administration) was considering technology that would allow airport security to "read the minds" of boarding passengers, in an attempt to prevent acts of terrorism. According to Frank J. Murray, "Officials of the National Aeronautics and Space Administration have told Northwest Airlines security specialists that the agency is developing brain-monitoring devices in cooperation with a commercial firm, which it did not identify" (A01). Interestingly, this was not the first attempt at mind reading for the purpose of data

gathering and crime prevention. The US Military conducted numerous experiments during the 1960s, 1970s and 1980s to develop mind reading capabilities (Garfinkel 234). One team reportedly discovered at least seven people that could reliably describe the thoughts and actions of people at a great distance (Garfinkel 234). The difference with the modern program is that it attempts to utilize science rather than psychic abilities.

In NASA's system, airports would mount devices designed to monitor the brain waves and heartbeat patterns of passengers into airport screening devices (Murray A01). If NASA is able to perfect this technology, then walking through a metal detector might subject an individual to more than just a scan for metallic objects. It might also subject an individual to a more encompassing scan, one that would take into account the individual's panoptic information. According to Murray, "Computers would apply statistical algorithms to correlate physiologic patterns with computerized data on travel routines, criminal background and credit information from 'hundreds to thousands of data sources,' NASA documents say" (A01).

Currently, NASA is not attempting to examine and decode actual thoughts, but rather search for biological patterns that match ones considered consistent with criminals in the moments before they commit a crime. According to Rick Mathieson, "In fact, the technology might one day be able to identify nuero-electric patterns associated with the way the brain functions when a person is planning to commit a crime" ("brain storm"). Specialists would analyze the biological information along with other personal information regarding the individual, to determine if the person is about to commit an act of terrorism. This is similar to the methods employed by a profiler or investigator, only the amount of information analyzed is much more extensive and very private, and the search is more intrusive. Personal actions that might signal a potential terrorist are a one-way plane ticket, changes in grocery shopping patterns

and changes in spending patterns. Biological signs would include accelerated heart rate, emission of specific brain wave patterns and certain signals conveyed by the eyes. According to Mathieson, "The idea is to quickly render a complete picture of an individual traveler and then run algorithms to assess the threat risk" ("brain storm").

NASA is developing the mind-reading technology as part of its role in developing improvements to the CAPPS (Computer-Aided Passenger Pre-Screening) system currently employed by airports. The September 11, 2001 hijackers used dry runs to test the current CAPPS system's ability to identify potential hijackers as threatening (Murray A01). According to Mathieson, "Presently, the CAPPS system collects and stores basic travel information – whether you bought your ticket with cash or credit card, whether you're a frequent flier, and when was the last time you flew" ("brain storm"). Many organizations are looking at ways to improve the CAPPS system, to improve airports' ability to prevent passenger related problems. The new system (tentatively named CAPPS II and discussed in the next section) could contain many improvements, including NASA's mind-reading technology.

The "mind reading" portion of the technology is actually relatively simple, and is based upon techniques presently available to medical professionals. According to Murray,

> "He [Herb Schlickenmaier, the NASA researcher who made the presentation to Northwest Airlines] likened the proposal to a super lie detector that would also measure pulse rate, body temperature, eye-flicker rate and other biometric aspects sensed remotely...he confirms that NASA has a goal of measuring brain waves and heartbeat rates of airline passengers as they pass screening machines" (A01).

In order to be effective, the scanners would need to use fMRI (functional Magnetic Resonance Imaging) to get a clear picture of the brain's current activity (Mathieson "brain storm"). In the

closing months of 2004, scientists proved that the brain looks much different in an individual who is lying, and displays a higher rate of activity (Reuters "Brain scans"). According to the Reuters story,

> "Lying caused activity in the frontal part of the brain --- the medial inferior and pre-central areas, as well as the hippocampus and middle temporal regions and the limbic areas. Some of these are involved in emotional responses, Faro said. During a truthful response, the fMRI showed activation of parts of the brain's frontal lobe, temporal lobe and cingulate gyrus" ("Brain scans").

The problem exists with performing the scans wirelessly and quickly (Mathieson "brain storm"). Current fMRI scanners are large and require an unacceptable amount of time for even the simplest scans of any body parts.

In addition, problems exist in identifying foolproof patterns that will not generate any false positives or false negatives. Thus far, scientists have not determined what signals the brain generates before committing a crime. An individual who just had an argument with their spouse, one who is feeling guilty over some minor act, who is having a bad day or thinking about how much they hate their boss, could emit brainwave patterns similar to those of a criminal about to commit a crime. It will require very careful analysis to determine brain patterns and background patterns that can absolutely prove that someone is about to commit a terrorist act.

NASA is invading the privacy of individuals before the system is even in place. According to Murray, "NASA also requested that the airline turn over all of its computerized passenger data for July, August, and September 2001 to incorporate in NASA's 'passenger-screening testbed' that uses 'threat-assessment software' to analyze such data, biometric facial recognition, and 'neuro-electric sensing'" (A01). Northwest Airlines cooperated in turning the

data over to NASA, and anyone who flew in the months prior to the September 11, 2001 attacks could have had much of their personal information analyzed as part of the process of developing different behavioral models. It is possible that the government could use the personal information as the starting point for a centralized database. According to Mathieson, "The concept may be part of the Bush Administration's plans for a 'Total Information Awareness' system, a global electronic dragnet designed to use data mining to look for threatening patterns in everyday transactions and information – your credit card purchases, student report cards, mental health records, and more – that is reported to roll out in 2007" ("brain storm").

This program further proves the government's quest for a centralized database of a perfected panoptic sort. If NASA plans to analyze biological information gathered in real-time at an airport with other pertinent personal information regarding an individual, then they must have access to the additional information.

CAPPS II

As mentioned in the previous section, the CAPPS II system seeks to correct problems in the original CAPPS system that allowed the September 11, 2001 terrorist attacks to occur. Putting aside NASA's mind reading experiments, the readily available features of CAPPS II mean that individuals booking a flight will expose their personal information to a greater degree than ever before.

The controversy surrounding the system first appeared when the government announced that when an individual booked a flight, the system would use public records to color-code the potential airline passenger as green, yellow or red. A "green" rating enables a potential passenger to fly without any extra measures; a "yellow" rating signals that a potential passenger will

receive additional checks at the airport; a "red" rating prevents the potential passenger from flying. According to Brock N. Meeks,

> "The new system, the cost of which isn't known but will be borne entirely by the federal government instead of the airlines, will take a traveler's personal information — name, address, date-of-birth and telephone number — and feed it into commercial databases and police records, the latter looking only for instances of violent crimes" ("TSA Defends").

After the commercial database check, the system would check the potential passenger's information against the government's database of known terrorists. According to Sara Kahaulani Goo,

> "...up to 8 percent of passengers who board the nation's 26,000 daily flights will be coded "yellow" and will undergo additional screening at the checkpoint, according to people familiar with the program. An estimated 1 to 2 percent will receive the "red" label, prohibiting them from boarding. These passengers also will face police questioning and may be arrested" ("Fliers to", A01).

Although the USG hoped to implement the new system by summer of 2004, opposition from the ACLU and the major airlines has slowed the system's progress. First, Delta Airlines, which was supposed to assist the government in testing the system, backed out in response to criticism and threats of a boycott from the traveling public (Goo, "Fliers to" A01). Next, the ACLU brought forth a lawsuit against the TSA (Transportation Safety Authority) to prevent the system's implementation. One of the ACLU's main complaints was that the system would create too many false positives, stripping innocent individuals of their basic right to travel freely. The system would not inform potential passengers of their color rating or allow them to view the

information used to determine their status, making it impossible for individuals to correct errors in their information and categorization.

The situation worsened upon the discovery that three of the major airlines (Northwest, American Airlines and JetBlue) had shared passenger information with the USG without passengers' consent. The fallout from the breaches was great, causing airline companies to change their privacy policies and practices to inform passengers of potential data sharing. According to Goo, "Major U.S. carriers are scrambling to create disclosure policies that inform customers they might share personal data with the federal government, in response to two highly publicized cases in which airlines secretly handed over private passenger information" ("Airlines Hustling" E01). While the legality of data sharing is questionable, consumer reaction was sharply negative. According to Goo,

> "Legal experts said there are no laws against companies sharing information with the government or other companies. But companies that do not disclose under what conditions they share the information and who gets it could face suits from consumers for deception and breach of privacy. They could also face fines or investigations by government agencies, such as the Federal Trade Commission" ("Airlines Hustling" E01).

Now, the FBI is holding onto the information gained from the airlines, refusing to share it or release it. According to an AP report, "The bureau is keeping 257.5 million records on people who flew on commercial airlines from June through September 2001 in its permanent investigative database, according to information obtained by a privacy group and made available to The Associated Press" ("FBI holds"). The story continues,

> "The data are called passenger name records, or PNR, and can include a variety of information such as credit card numbers, travel itineraries, addresses, telephone numbers

> and meal requests. David Hardy, the FBI's chief of the record/information dissemination section of the records management division, said in a legal document dated Jan. 5 that the data were being stored and combined with other information from the Sept. 11 investigation, dubbed PENTTBOMB" ("FBI holds").

This provides additional proof that the USG is attempting to construct a large, centralized data warehouse for the purpose of any number of privacy invading projects.

Despite new attempts at securing air travel, the system is still vulnerable to unsophisticated, low-tech attacks. In September 2003, an individual packaged himself in a shipping crate, registered it as containing computer equipment and was flown cargo-class from New York to Dallas (Koeing "Shipping clerk"). In February 2004, a man strolled past two security checkpoints and onto a jumbo jet without a ticket at Las Angeles International Airport during a period of time when the nation was on high alert (MSNBC "Brazen intruder").

In April 2004, the ACLU announced a lawsuit against the TSA for the CAPPS II system, nicknamed by the media as the "no-fly list". The ACLU is representing a number of passengers who believe that the system improperly subjected them to additional questioning or caused the denial of their flight privileges. One individual, David Nelson, believes that his case is one of mistaken identity, and the government should be looking for another David Nelson (WJLA "ACLU sues"). Due to the level of outcry from citizens and activist groups, on July 15, 2004 the TSA announced that it had cancelled the CAPPS II program.

Smart Stamps

The USPS (United States Postal Service), losing money for years due to the growing popularity of eMail and instant messaging, is looking for a way to increase revenues without continuously raising the price of stamps. Unfortunately, part of their plan involves stamps

embedded with tracking devices that would allow the USPS to track a particular stamp's movement throughout the postal system.

According to Alorie Gilbert, "Thought details remain sketchy, an intelligent mail system would involve using barcodes or special stamps, identifying, at a minimum, the sender, the destination, and the class of mail...It [the report suggesting the changes] also suggests USPS work with the U.S. Department of Homeland Security to develop the system" ("Postal ID").

The smart stamp plan has many opportunities for abuse. The USPS claims that one of the biggest uses of smart stamps would be to track communication between individuals, in order to link them to one another. Of course, the USPS wants everyone to believe that those individuals would be under surveillance for a legitimate purpose (suspected terrorists). Perhaps earlier implementation of a smart stamp system would have enabled authorities to capture the Unabomber or the individual responsible for the anthrax-tainted mailings after September 11, 2001. The problem is that we have no way of limiting or monitoring the government's usage of smart stamps. Nor do we know what personal information the USPS will connect to each stamp.

If the USPS can use the smart stamps to monitor communications between suspected criminals, then what would prevent the government from monitoring each letter that every individual ever sends? The information could be stored along with all of our other panoptic information, ready for use or sale. After all, the USPS has a history of information sale and misuse. According to Garfinkel, "...the National Change of Address Program [used for mail forwarding when an individual moves] is actually run by the same companies that send tens of billions of pieces of junk mail each year to hundreds of millions of American consumers" (157). Garfinkel explains, "When you fill out a change of address card, the card is sent to a processing center where the information is typed into a computer and then transmitted to the nation's largest

direct marketing firms" (164). The problem is that once the data is in the hands of those firms, it is nearly impossible to assure proper use. According to Miller, "Most direct merchants generate subsidiary income from selling the names in their database to other companies..." (309). Whether your name gets to marketers through sale or through the National Change of Address Program, the result is usually the same: Uncontrolled sale and misuse of your personal information.

FBI's DNA Databank

The FBI plans to make a collection of blood samples of all federal inmates and parolees. Minimally, the FBI desires samples from criminals convicted of violent crimes, mainly rape. Of course, state and federal law enforcement agencies will not stop with just sex offenders. According to Garfinkel, "Some states require that all convicted violent criminals provide samples. Others require that people convicted on nonviolent crimes be genetically fingerprinted as well. Some states even collect and databank the genetic patterns from people accused of crimes" (53). Under the DNA Analysis Backlog Elimination Act of 2000 [Public Law 106-546], federal inmates and parolees were required to provide blood samples for the FBI's collection. The FBI cataloged the samples, added them to the collection and made the collection available to law enforcement agencies across the nation. Thankfully, the Court of Appeals determined that the blood sampling procedures were unconstitutional. According to David Kravets, "The 9th U.S. Circuit Court of Appeals ruled that requiring the blood samples was illegal because they are taken without legal suspicion that the convicts were involved in other crimes" ("Federal appeals"). According to Kravets, "Knox [Monica Knox, a deputy public defender of Los Angeles] said the government has extracted blood from thousands of federal inmates and former

prisoners on supervised release. She said the decision, if it survives appeal, could also nullify state laws that require the taking of blood from inmates" ("Federal appeals").

It is fascinating to witness the government and law enforcement repeatedly attempt to stretch technology and public policy to fit their current needs. The DNA databank was probably illegal and somewhat evasive when it only involved criminals convicted of violent crimes. Then they decided to apply it to those convicted of non-violent crimes and those only accused of crimes. This is the "mission creep" scenario that concerns experts every time the USG passes a new law or adopts a new technology.

US VISIT

The US VISIT (United States Visitor and Immigration Status Indicator Technology) program seeks to identify individuals entering the US from another country. While there is a valid argument for such a program, the extent to which US VISIT identifies and monitors individuals is an invasion of their privacy.

According to Fisher,

> "As part of the process, foreigners arriving at US-VISIT-capable airports and seaports have each of their index fingers scanned and a digital photo of their faces taken. This data is stored in a database, along with the person's visa number, and compared against so-called watch lists of known terrorists and criminals. Each time the person enters the country, another database search is done to see if any new information about the visitor has accumulated since his or her last visit" ("New DHS").

Visitors will also be checked when they leave the country, to verify that they obeyed the policies of their visa (MSNBC "Airports to"). Reports estimate that the program will check 24 million

visitors per year (MSNBC "Airports to"). By the end of 2004, the USG hopes to have the program available at 50 land crossings along the US border (MSNBC "Airports to").

Privacy Protection Laws

A thorough and proper examination of the legal landscape must include privacy protection laws. Unfortunately, many of the privacy protection laws are relatively new, and have not generated the publicity of the laws that invade privacy. In addition, the USG is not nearly as concerned with enforcing laws protecting privacy as it is with enforcing invasive laws. For these reasons, it is difficult to examine the results and possible success of these laws. The following paragraphs examine each law and the available results thus far.

The goal of FCRA (Fair Credit Reporting Act; 15 USC §1681) was to provide consumers with the tools necessary to gain knowledge of their credit information, and to protect their information from improper sale or use. Unfortunately, enforcement of FCRA is loose and the penalties are weak. Credit bureaus regularly ignore consumers' complaints regarding incorrect information in their credit file. Some experts attribute the growing threat from identity theft to creditors' and bureaus emphasis on selling credit protection products and services rather than altering their own processes to prevent identity theft from occurring. Enforcing the guidelines put forth by the FCRA would reduce the threat from identity theft. We need a greater sense of responsibility and accountability from financial institutions and credit bureaus to provide proper backing for the law. If a consumer has a justifiable complaint regarding their credit file, all credit bureaus should have to take notice and correct the error or face legal consequences. Unfortunately, Michael E. Staten and Fred H. Cate (2004) discovered that experts cannot agree on the definition of an "accurate credit report", or whether the current credit reporting system properly represents consumers. Garfinkel claims that the only way to properly enforce privacy

laws, especially the FCRA, is through stiff financial penalties against all organizations that misuse information ("Database Nation").

The goal of FERPA (Family Educational Rights and Privacy Act; 20 USC §1232g) was to protect students' rights and the privacy of their personal and academic information. To this date, there has been minimal compliance with FERPA, mainly due to a lack of enforcement and understanding. Matt Rose and Dhazi Yang (2004) found that many educators cannot readily identify the type of student information to which FERPA applies, especially in regard to computer usage. A study of FERPA at various educational institutions, including Stanford and MIT (Massachusetts Institute of Technology), found that many higher education institutions are not vigorously following FERPA's guidelines (Anonymous "A study"). In addition, many institutions do not have clauses in their Privacy Policy to protect students' information and institutions that do have privacy protection statements in their Privacy Policy often violate those statements in their practices (Anonymous "A study").

Unfortunately, the Pentagon is one of the worst violators of the rules enacted by FERPA. According to Robert L. Flanigan, "To boost recruitment numbers in a time of war, the Pentagon is working with a private marketing firm to help compile a database of potential recruits as young as 16 — using Social Security numbers, e-mail addresses, grade-point averages, ethnicity and other personal information" ("Military culls"). The military admits to striving towards the goal of creating a "centralized database" maintained by the DoD, which would also include information retrieved from Department of Motor Vehicles records (Flanigan "Military culls"). The Pentagon gained the right to gather the information from the NCLB (No Child Left Behind Act of 2001; PL 107-110), which directly contradicts the provisions set forth by FERPA. Under NCLB, the Pentagon may collect a student's information, unless their parents or guardian

specifically chooses to deny the Pentagon access to their child's information. Fairport School District, located in Fairport, NY, is one of a handful of districts nationwide that has chosen to restrict the military's access to student records, at the threat of reduced funding from the government. Better oversight and enforcement is necessary to guarantee FERPA compliance and the protection of students' information. In addition, Congress must repeal the sections of NCLB that enable the Pentagon's data gathering practices.

The goal of HIPAA (Health Insurance Portability and Accountability Act of 1996; Public Law 104-191) was to protect patients' rights concerning their medical records and provide better oversight and regulation for the health insurance industry. A survey conducted by AHIMA (American Health Information Management Association) revealed that 70% of respondents had uncovered privacy issues in their organization after they began following HIPAA's guidelines (NewsRx.com "Survey"). Like many laws that provide sweeping guidelines regarding privacy, information management and financial regulation, HIPAA is complex, and many organizations find compliance difficult. However, if this survey provides any indication of future results, then HIPAA has been beneficial in protecting personal privacy.

The goal of COPA (Children's Online Privacy Protection Act; 15 USC §6501-6506) is to protect children while they are online. The act was highly controversial and heavily debated from its very beginning, as many experts felt that it went too far in censoring the content available to adults. Early on the law suffered numerous defeats and revisions in the court system before becoming effective. The main benefit of COPA was that organizations were required to obtain a parent or guardian's permission before collecting information from individuals under the age of 13. Unfortunately, enforcement of that policy has been non-existent, and most Web sites

"comply" by simply displaying a checkbox that the user checks if they are over the age of 13. With no way to truly verify the age of the user, the policy is useless.

The goal of GLB (Gramm-Leach-Bliley Act of 1999; Public Law 106-102) was to regulate the manner in which financial institutions collect and share an individual's personal information. Many privacy advocates have spoken out against GLB because of its numerous loopholes and inadequate privacy protection clauses. One of the main criticisms of GLB is that it requires individuals to opt-out of information sharing, rather than requiring them to opt-in before organizations share the individual's information (Stephen Brostoff 42). In addition, GLB allows each state to pass its own laws restricting financial institutions' information sharing, potentially creating a confusing legal landscape of contradicting laws (Brostoff 42). For these reasons, privacy advocates are calling for a stronger law at the national level to replace GLB.

The goal of Sarbanes-Oxley (Sarbanes-Oxley Act of 2002; H.R. 3763) was to regulate the operations of all publicly traded companies. The law's creation resulted from the financial disasters created by the recent slew of accounting scandals, including Enron and WorldCom. Although not specifically designed to protect individual privacy, the enforcement of SOX has resulted in better privacy protection, through improved security, process management, training, document management and increased use of encryption. Unfortunately, few companies are complying with Sarbanes-Oxley, making it impossible to determine the results of the law's sections regarding privacy protection and information sharing.[14]

The goal of CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003; S.877) was to reduce and prevent the onslaught of spam eMail that invades most users' inbox on a daily basis. Many organizations are now reporting that 75-80% of

[14] The law implements a graduated compliance deadline that requires only organizations with the highest level of annual revenue to comply at the first deadline (June 2004). Organizations in the middle and bottom revenue brackets have more time to reach compliance. In addition, only publically traded companies must comply with SOX.

the eMail messages that they receive daily are spam. Individuals are receiving hundreds of spam eMail messages daily. The threat to privacy from spam is from how the spammers accumulate eMail addresses, and the dangerous phishing attempts that spam often carries.

Spammers may retrieve eMail messages through "harvesting", where a "robot" program makes its way around the Internet, grabbing eMail addresses from Web pages and Newsgroup messages. This has spawned two popular methods of tricking the robot list gatherers: "my_address@myispREMOVE-THIS-LAST-PART.com" (the robot will not remove the capital letters in the address but a human would) and "my_address at myisp dot com" (the robots do not recognize this as an eMail address because it does not contain an @ sign. A human would recognize the use of phonetics and properly use my_address@myisp.com). In some cases, spyware and viruses are responsible for stealing an individual's eMail address. Many times, an individual signs up for a mailing list and the list owner sells the list to another organization. The purchasing organization often sells the list to another organization. This pattern may continue endlessly. Occasionally, employees gather eMail addresses through theft. In 2004, AOL charged a former employee with stealing the company's entire subscriber list, which amounted to 30 million consumers and 90 million screen names (Sullivan "AOL customer"). He then sold list to a spammer, who sold the list to another spammer.

A few lawsuits have been filed under the guidelines of CAM-SPAM, although only one has reached a verdict. A jury found Jaeremy Jaynes guilty of violating CAN-SPAM, and recommended a 9-year prison term (the judge has not delivered the final sentence). Jaynes was one of the world's most prolific spammers through the 1990s, sending 10 million eMail messages per day and generating revenues of $750,000 per month (AP "Trial shows"). Authorities estimated Jaynes' net worth at the time of his arrest at $24 million dollars.

Although it is far too early to judge CAN-SPAM, critics believe that the technological and personnel resources are not available to properly enforce CAN-SPAM. Most also believe that the act is not well-constructed to properly define and prosecute spam. In addition, most experts believe that technology, not legislation, is the key to preventing spam eMail messages. Ultimately, it will take a combination of legislation and technology to prevent spam from saturating network bandwidth worldwide. However, CAN-SPAM is an attempt by the government to protect individual pricy by protecting eMail addresses, personal information, and by preventing phishing attempts from reaching their recipients. Even if many experts consider the act shortsighted and toothless, it is a step in the right direction.

Summary of Government Policies

We should not be surprised that members of the government would strive to undermine individual privacy, as a recent report disclosed that government officials have been spying on each other for over a year. According to Charlie Savage, "Republican staff members of the US Senate Judiciary Commitee [SIC] infiltrated opposition computer files for a year, monitoring secret strategy memos and periodically passing on copies to the media, Senate officials told The [Boston] Globe" ("Infiltration of"). For at least one year, Republican staffers exploited a computer glitch that provided them access to protected Democrat documents without the required passwords, known only to members of the Democratic Party. According to Savage, "...they were able to read talking points and accounts of private meetings discussing which judicial nominees Democrats would fight -- and with what tactics" ("Infiltration of"). If we cannot trust members of the government to maintain a sense of legality and ethics in their dealings with each other, then we definitely cannot trust them in their dealings with individual

citizens. In this "Information Age", the value of closely guarded information has grown far beyond the capability of ethics and the legal system to guarantee its protection.

Even the most rational experts are beginning to fear the government's ability to monitor its citizens. In a commentary for CNET's News.com, security expert Bruce Schneier discussed the threats looming against residents of the US. According to Schneier,

> "In December, a provision slipped into an appropriations bill allowing the FBI to obtain personal financial information from banks, insurance companies, travel agencies, real estate agents, stockbrokers, the U.S. Postal Service, jewelry stores, casinos and car dealerships without a warrant--because they're all construed as financial institutions. Starting this year, the U.S. government is photographing and fingerprinting foreign visitors coming into this country from all but 27 other countries" ("Slouching toward").

Schneier continued,

> "When you put the police in charge of security, the trade-offs they make result in measures that resemble a police state... The laws limiting police power were put in place to protect us from police abuse. Privacy protects us from threats by government, corporations and individuals. And the greatest strength of our nation comes from our freedoms, our openness, our liberties and our system of justice" ("Slouching toward").

We must carefully consider the words of experts like Schneier, whose work has defined the core values of digital security. When the experts begin to question the government's actions, the residents of this country must take notice. We must be aware of threats from public policy, and we must use our democratic system to fight back against them.

Results of Policy Enactment

One only needs to examine the current landscape to witness the effects of legislation on their lives. A sign erected by the entry area of the Lake George, New York steamboat rides states the following: "Our Security Measures include taking a photograph of ALL boarding passengers. While these photos are available for purchase, you are under no obligation to purchase them. Due to our heightened Security Requirements and for everyones' [SIC] safety, all bags and carry-on items are subject to search". Is it necessary to photograph every passenger boarding a steamboat on Lake George, or is this a thinly veiled attempt by the steamboat operators to reposition consumer annoyance at an unnecessary sales pitch on the USG? Whichever the case, this is one example of a situation where public policy and current events have radically altered the landscape of our society.

History shows that we must prevent our panoptic information from becoming the property of the government and law enforcement officials. According to Garfinkel, "In February 1999, the South Carolina Public Safety Department sold photograph's of the state's 3.5 million drivers to Image Data LLC of Nashua, New Hampshire. The price was a bargain basement of $5,000, or roughly a penny for seven photos, according to an article in the *Washington Post*" (61). During World War II, the Census Bureau provided the War Department with detailed lists of the names and addresses Japanese-Americans living in the US (Garfinkel 228). In the 1950's, the FBI conducted surveillance against Communists and homosexuals throughout the US (Garfinkel 228). During the 1960s and 1970s, the FBI infiltrated women's groups, black groups, environmental groups and gay groups on college campuses (Garfinkel 228). Garfinkel nicely summarizes the controversy surrounding government invasions:

"The problem is that the FBI, and the country at large, have shown a willingness to get caught up in the issues of the day and unfairly target, prosecute, and imprison individuals for what they say and believe, rather than for what the actually do. This makes it very difficult to respect the FBI's claims that aggressive new technologies and mandates are required for tracking and stopping terrorists and murderers" (228-229).

The threats discussed in this section are numerous. Each policy and program by itself presents a disturbing threat to individual privacy, and their combined threat provides an unprecedented level of power to a select few of the highest-ranking individuals in the USG. This section discussed a few policies designed to protect individual privacy, unfortunately they are either poorly enforced, or too newly ratified to have shown true effectiveness. For this reason, the discussed policies and programs raise the Privacy Level Indicator to 4.25. The only thing preventing the Indicator from reaching the maximum level of 5.0 ("Uncontrolled") are the few privacy protection laws presented at the end of this section. If those policies receive additional funding and better enforcement, they could slow the Bush Administration's current trend of trampling individual privacy. However, it must be reinforced that the policies and programs discussed in this section provide the USG with the authority to perform an unending panoptic sort. Our society is on the brink of a crucial moment in history. As we put more time and distance between September 11, 2001 and the present, the USG must relax its invasive legislations. It is critical to rethink many of the policies and programs discussed in the following sections, to determine if they provide relevant protection compared to their invasion of individual privacy.

Non-computer Technology Section

Automobile Data Recorders

Data records, a staple of airplanes for decades, are making their way into automobiles. Automobile manufacturers currently have EDRs (Event Data Recorders) installed in approximately twenty-five to forty million automobiles in the U.S. (Don Oldenburg "The snoop"). According to David Coursey, "The NHTSA [National Highway Transportation Safety Administration] estimates that 40 million crash data recorders have been installed in vehicles sold in the U.S., representing about 20 percent of vehicles on the road today" ("Is your"). Most consumers do not realize that their automobiles contain the devices (used primarily by law enforcement and automakers for crash investigation and safety improvements). According to Oldenburg, "A 2002 survey by the Insurance Research Council found that two-thirds of car buyers didn't have a clue about the data recorders" ("The snoop"). According to Coursey, "The automakers kept the existence of these crash data recorders...secret until 1999, when a GM executive revealed their existence (perhaps unintentionally) in a speech" ("Is your"). The EDRs found in current automobiles do not record the same volume of information as their airplane counterparts. Engaged by the same circuitry that engages the airbags, EDRs record mainly crash-related data.

EDR implementation varies between automobile manufacturers. According to Oldenburg, "GM, a leader in EDR technology, has been installing the nondescript silver devices in its air-bag-equipped vehicles since 1974...Ford Motor Co. has EDRs in all cars, light trucks and SUVs manufactured in North America since the 2002 model year. Only Mercedes has taken a public stance against EDRs, stating that they have an extremely intelligent EDR device waiting for

implementation in vehicle models, but the company has decided to wait until society and law enforcement better grasp how to handle the situation" (Oldenburg" The snoop").

The recent release of retail EDR devices has intensified the discussion of the devices. Road Safety International developed one consumer EDR device to allow parents to monitor their children's driving behavior (Oldenburg "The snoop"). According to Oldenburg,

> "The modular components record data, such as seat-belt-use, speed, hard braking, hard cornering, pedal-to-metal acceleration and throttle positioning, that can be uploaded to home computers using software that analyzes driving performance...But that's only the beginning: In three months, an under-$200 global positioning system accessory will be available to record where the car goes...Next year, the communications module will allow parents to locate their teen drivers on an online map in real time".

If parents' lack of trust in their children is not reason enough to despise these devices, then consider some of the other problems. If the EDR device has wireless capabilities (which it will in order to enable real-time transmission of the car's location to an online map), then it suffers from the weaknesses and threats facing all wireless devices.[15] Another issue surrounds the security of the online map that parents can use to track their children. Road Safety must assure that the company's employees properly secure the Web Site against crackers or unauthorized access. In addition, one must question whether anyone will certify the devices, test them and prove that they only beam information to the specified location. Otherwise, the user has no idea if the device is beaming information to the government for use as profiling data, or if Road Safety International is selling information transmitted by the divide to third parties interested in users' travel and driving habits.

[15] This thesis discussed wireless devices earlier.

Cellular Phone Tracking

Currently, it is difficult or impossible to track the location of a cellular phone within a reasonable proximity. This will change, as cellular phone providers ready E911 (Enhanced 911) systems. The E911 initiative forces cellular phone manufacturers and service providers to build location-aware 911 capabilities into their phones and service networks. Recent situations in which individuals called 911 from their cellular phones but 911 operators could not determine their location, accelerated E911 implementation. E911 is a reasonable and necessary feature to enhance the ability of cellular phones to provide assistance in an emergency. The problem is that users desire control over when someone is tracking their phone.

The capability and legality of cellular phone tracking varies between countries.

> "Finland has proposed a new law that would let parents track the movements of their young children via mobile phone, even without their consent, in a move that could set an EU benchmark in privacy and handset use...According to the draft, individuals aged 15 or older could only be tracked after giving their consent, but for children under 15 such consent could also be given by their parents or guardians" (MSNBC "Finns ready").

Finland is the most advanced country in the world in cellular phone technology and has the greatest cellular phone penetration per capita. If passed, this law would also make Finland a world leader in testing the waters of cellular phone tracking and the privacy issues surrounding phone tracking. If instituted, this law sets a dangerous precedence in setting privacy rights for children. However, the issue of children's privacy and safety is a delicate issue, and safety often takes precedence over privacy. This is most obvious in school districts, which often trample students' right to privacy in order to provide them with a safe and healthy learning environment.

RFID

RFID (Radio-Frequency Identification) chips are part of a computing domain known as "passive computing", in which a device with no computing intelligence can interact with and provide information to a larger computing system. According to Alorie Gilbert and Richard Shim, "Radio frequency identification (RFID) technology uses microchips to wirelessly transmit product serial numbers to a scanner without the need for human intervention. ("Wal-Mart cancels"). The first RFID devices were small rectangular plastic sensors still found in many CDs and DVDs in retail stores. Newer technology has allowed manufacturers to develop RFID devices roughly the size of the fingernail on the average human's pinkie finger.

The manufacturing industry is excited at the prospect of RFID, as the technology will allow manufacturers to control and automate their processes in ways that were previously impossible. "Smart warehouses" are being designed that will allow the tracking of RFID-enabled products from manufacture and assembly to delivery, enabling more efficient operations. Eventually, automated forklift devices will use RFID tags embedded in products to find a product on warehouse shelves and deliver it to the shipping department. In addition, RFID will allow manufacturers to monitor in real-time their current inventory, enabling them to better adjust their just-in-time operations.

The problem with RFID devices is that they open the door to monitoring and tracking consumers through the products they purchase. According to Garfinkel, "Like other identification systems, RFID system's don't actually identify a car, a pet, or a person: they simply identify the tag. And since no cryptography is employed by today's RFID systems, an RFID identification response can be eavesdropped, falsified, or otherwise forged" (80). A product that contains an RFID chip could allow a retailer to track the consumer's movement

throughout the store, and possibly beyond the store's limits. According to Garfinkel, "The tags can also be read without the owner's knowledge. Since today's tags have no memory, there is no way to determine how many times a tag has been read..." (80). Gillette and Wal-Mart had planned to test a "smart shelf" system that would allow the tracking of RFID products from the minute they left the display shelf until the moment they left the store. The trial was to determine if RFID enabled products could prevent shoplifting and assist customer associates in finding items that customers place back onto the wrong shelves.[16] Reaction to the planned trial from consumer privacy groups was extremely negative, and Wal-Mart abruptly cancelled the trial before it began, although Gillette continued with similar plans in stores throughout Europe (Gilbert and Shim, "Wal-Mart cancels"). C.A.S.P.I.A.N (Consumers Against Supermarket Privacy Invasion and Numbering), against RFID devices since their introduction in supermarket "consumer loyalty" tags, was especially vocal in calling for Wal-Mart to cancel the trial. In addition, economics may have played a part in the decision, as RFID devices currently cost about 10 cents apiece, which would cut hard at Wal-Mart's slim profit margins in the retail superstore industry (Gilbert and Shim, "Wal-Mart cancels"). C.A.S.P.I.A.N's boycott threats also caused Italian clothier Benetton to cancel a trial in which the company would have sewn RFID devices into their clothing (Gilbert and Shim "Wal-Mart cancels").

Unfortunately, Wal-Mart's decision to cancel the "smart shelf" trial was only a decoy to draw attention away from another RFID trial. According to Gilbert, "Wal-Mart Stores and Procter & Gamble quietly tested a controversial new retail technology earlier this year that allowed P&G employees to observe shoppers via a Webcam as they removed cosmetics from shelves, representatives of both companies confirmed Friday" ("Smart Shelf"). The test, conducted in the suburbs of Tulsa, Oklahoma, proves that manufacturers and retailers cannot be

[16] Shoplifters target Gillette's Mach 3 razor blades more than any other product.

trusted with RFID or other forms of tracking technology. Not only did they secretly use RFID chips to track product movement, they used a Webcam to spy on innocent shoppers without their consent. Proctor and Gamble claimed that the Web cam allowed the company to confirm the accuracy of the data data generated by the smart shelves (Gilbert "Smart Shelf"). If this were truly the case, then Wal-Mart and Proctor & Gamble should have posted signs near the shelf specifically detailing the test and the presence of the Webcam, as well as releasing information to the media beforehand. Proctor & Gamble cited the existence of a sign posted near the shelf informing customers that electronic monitoring was present, although the sign did not specifically mention the existence of chips embedded in the product packaging or the Webcam (Gilbert "Smart Shelf").

Gillette's European RFID trials with retailer Tesco also crossed the line of privacy invasion. According to Andy McCue, "But privacy groups started protesting outside the Tesco store when it emerged that the supermarket was automatically taking photographs of shoppers when they picked the blades off the shelf and when they left the shop with any tagged product" ("Gillette shrugs"). Once again, a retailer proved that they would not stop with simply tagging products for inventory management purposes. Instead, they used the RFID as part of a scheme to spy on consumers while they shopped.

Supporters of RFID point to the fact that the devices currently used in inventory and retail have an effective range of a few inches. The problem with that theory is that it does not consider other current or future applications. It is critical to halt a dangerous technology in its infancy, before it has gained maturity and advanced capabilities. It is true that devices used in stores only have a short range, but RFID devices used for other purposes have much longer range. In addition, the short range of RFID devices is only a valid argument if the cashier

properly disables the devices during checkout. It is common to see an individual trigger a store's doorway mounted RFID scanners while entering a store for the first time. This happens because the cashier in the previous store did not properly disable the RFID tags during checkout. In the future, this could lead to a situation similar to tracking cookies, where one company creates RFID tags for purchase by retailers. Rather than being disabled at checkout, the devices would remain active, to track which stores a consumers enters, and in which order. This would provide valuable marketing data for retailers.

An example of such a device is the EZPass system. EZPass is an RFID device, slightly smaller than a CD case that the user attaches to the windshield of their automobile. The device allows the user to drive through EZPass equipped tollbooths without stopping. The system automatically charges the proper toll amount to the credit card the user supplied when they signed up for their EZPass account. The first problem with the EZPass system is that the technology employed allows the reader to contact the windshield-mounted RFID device from 10 feet away or slightly further. Eventually RFID devices mounted in product packaging will achieve that level of sophistication. Then consumers will truly have to worry about retailers and manufacturers tracking them, or crackers finding unauthorized ways to activate the tags. Consider a kidnapper using the tags in a child's clothing, the same tags parents purchased to keep their child safe, to track the child and determine when they are alone.

In addition, the EZPass system proves that RFID-enabled devices set a dangerous precedent in their ability to collect information. The information recorded by the EZPass system includes the user's ID number, location of the tollbooth and the time and date that the vehicle passed through the tollbooth. Law enforcement officials could misuse this information by issuing

speeding tickets. It could be determined if a traveler was speeding by comparing the time it took a vehicle to travel between two tollbooths with the distance in miles between the tollbooths.

For-profit organizations are not the only ones interested in RFID, as libraries are considering the technology to streamline the process of borrower checkout. According to Joe Garofoli, "The San Francisco Public Library is ready to spend $1 million on technology that would make it easier to check out and track its collection and reduce costly workplace-related injuries...The tracking devices are called radio-frequency identification computer chips, RFID for short." (A-20). RFID tags will benefit librarians, but at a cost to consumers' privacy. Consider a scenario where someone has just recently discovered that they have a fatal illness, such as AIDS (Acquired Immunodeficiency Syndrome). They have not yet disclosed this to anyone, and are reading books and magazines on the disease and its treatments. Someone examining the individual's library records could determine that they have the disease, and even come close to pinpointing the time when the individual learned they had the illness. Or, situations could occur where a strange coincidence might cause police to be suspicious of an innocent individual. In addition, it is important to understand that RFID tags are a new technology, and eventually someone will discover a way to gain access to RFID chips outside of their intended scanner. In the future, what will stop FBI agents from sitting in unmarked vehicles across the parking lot or street from libraries, examining the books an individual just checked out? Just imagine if the technology was this advanced when the September 11, 2001 tragedies occurred: Agents could discreetly examine the books borrowed by every person of Middle Eastern descent at every library in the country, without alerting the individual or the librarian. This would enable a completely new level of racial profiling. If it does not seem possible,

consider that the technology advances daily: The RFID devices being considered by the San Francisco Public Library can be read from up to 3 feet away (Garofoli A-20).

Another danger from RFID is wearable ID badges required in many organizations, especially educational institutions. Teachers commonly have to wear ID badges with their name and photo in plain sight. The dangerous aspect of these badges is their potential for misuse. ID badges are often bar coded with information about the individual depicted on the badge, for use in the school's library or cafeteria. The problem is that districts could implement systems that would allow remote scanning of the bar codes. A district would only need to specify that an individual wear their badge on the outside of their body in plain site. The district could then place sensors around its schools, or in front of certain key areas (exits, bathrooms, lounges, computer labs or any other area of concern) to track the movement of individuals throughout the building. The information could automatically be stored in a data warehouse and mined by automated mining programs or manually by humans. This would allow the district to determine the habits and patterns of individual teachers. This information could determine if a teacher takes "too many" trips to or spends "too much" time in the bathroom, lounge, computer labs or outside. The district and administration in question determine what defines "too many" and "too much", which is a potential for information abuse beyond the fact that the school would be tracking its teachers. One only needs to consider that students could also be required to wear similar badges, which increase the threat posed by ID tags.

As more devices become RFID enabled, the threat from government intrusion increases. If the government can gain access to the data collected by an individual's RFID devices and credit cards, they can track that individual with startling accuracy. According to Guy Kewney, "Amalgamate the data from the bank with the data from Exxon with the data from a transit

system. Then add a loyalty card system, a mobile phone payment network, and a Government ID card system. The result: the State can track every citizen with far, far more detail than a simple RFID tracker could ever manage".

Security and privacy companies have begun working on products that will help alleviate consumers' privacy tag fears while allowing organizations to implement RFID-based solutions. RSA, known for its expertise in encryption technology, created an RFID "Blocker Tag" that prevents RFID devices from being properly read. The blocker tag sends signals to the RFID reader that prevents it from reading nearby tags (Fisher "RSA Keeps"). RSA is working with retailers to develop bags equipped with the blocker tags (Fisher "RSA Keeps"). After checkout, the sales associate would place the consumer's merchandise in a bag equipped with a blocker tag, reassuring the customer that the retailer is no longer querying the tagged merchandise. Solutions such as RSA's blocker tag are critical to the success of RFID at the retail level. Only by reassuring consumers that their privacy is being protected can RFID make its way into store shelves. The blocker tag does not protect the consumer once they return home and dispose of the bag, but that will not be a problem until RFID devices greatly overcome their distance limitations.

To answer these concerns, researchers at MIT (Massachusetts Institute of Technology) started the Auto-ID Center (http://www.autoidlabs.org/) to develop technologies and procedures to build consumer confidence in RFID. One product they are developing is a "kill command" or "kill switch" which would permanently disable the RFID device upon a product's scanning at the checkout register. In addition, they are developing a code of conduct for manufacturers and retailers to follow in implementing RFID. As with other similar technologies, the key is to provide proactive and open information to the public. Wal-Mart's secret RFID trials were a

major setback for RFID, Proctor & Gamble and Wal-Mart. Retailers should inform consumers when they enter the premises that RFID enabled devices are present in the store, so that each consumer may decide if they still desire to enter the store.

> State legislatures are also considering the future of RFID. According to Jane Black, "On Feb. 24, the Utah House of Representatives passed a bill mandating clear labeling of any product in which an RFID chip is embedded. A bill introduced on Feb. 27 in the California Senate goes further, arguing that retailers should need consumers' permission...The new [California] bill requires any business or state agency that uses an RFID system to track products and people to follow three rules. First, tell people that RFID is tracking and collecting information about them. Second, get express consent from customers before doing that. Third, detach or destroy tags before the customer leaves the store" ("Shutting Shopping").

Customer "Loyalty" Cards

Many stores now require their customers to use "loyalty" cards at checkout to receive advertised discounts. The cards, small enough to fit easily on a keychain, contain a barcode that the cashier scans upon checkout. The barcode is linked to the customer's account when they enrolled in the program. Scanning the card at checkout enables the store to track each customer's purchases. Retailers claim that the cards benefit consumers, because it enables stores to offer individual coupons to customers based on their previous shopping history. Some stores print out coupons with the receipt for items that the customer just purchased, or has purchased in the past.

The issue with loyalty cards revolves around information tracking and security. Most supermarkets and pharmacies require their customers to use the cards if they want to receive advertised discounts. This enables retailers to create a database containing all of their customers

and their purchases. Any time a database exists, there is potential for misuse, resale, government intrusion or data theft. C.A.S.P.I.A.N. has fought diligently against the cards, and tracks every instance of their misuse. In one case, law enforcement officials accused a firefighter of arson while investigating the fire that destroyed his home when they found a charred "firestarter" from Safeway (C.A.S.P.I.A.N. "News"). They used the purchasing information maintained by Safeway's loyalty card program to determine that he had recently purchased the item at the store (C.A.S.P.I.A.N. "News"). Authorities later dropped all charges against the firefighter when his wife confessed to the crime (C.A.S.P.I.A.N. "News").

The data warehouses resulting from loyalty cards also threaten privacy and can result in identity theft, if they are not secured properly. Katherine Albrecht, director of C.A.S.P.I.A.N., discovered a flaw in the design of CVS' Web Site that enabled the retrieval of customers' shopping information by entering the card number, their zip code and the first three letters of their last name (MSNBC "CVS pulls"). Although she was not able to obtain prescription records, Albrecht was able to obtain a record of all other purchases, including condoms and birth control (MSNBC "CVS pulls"). Albrecht has long been an opponent of the card programs, often citing their threat to privacy, as well as their influence on price increases (Albrecht "Supermarket Cards").

The threat from loyalty cards increases daily, as more companies adopt loyalty card programs, and endlessly grow their data warehouses. The threat of intrusion, from the government or crackers, makes these programs dangerous. Retailers must be convinced to cease loyalty card programs before we experience a compromise of a large retailer's data warehouse.

Chip Implants: Voluntary...For Now

Applied Digital Solutions, the company that gained attention two years ago with its wearable chip named the "Digital Angel", has developed a new implantable chip named the "VeriChip", which the company is currently testing in Mexico. The company chose Mexico as a test site for the new chip because a high level of kidnappings and robberies victimizes the country.

Current implementations utilize the chip as a means of creating a centralized database containing all of the user's medical information. Every chip contains a unique serial number that doctors and hospitals can use (if they have the necessary scanning equipment) to discover medical information regarding the individual. This system is especially useful in emergency rooms or ambulances, where patients are often unable to answer for themselves, and doctors often are unaware of the patient's medical history. The FDA (Food and Drug Administration) maintains that they will not regulate the implants, as long as the medical information is not contained directly on the chip.

Currently, Applied Digital Solutions does not have the ability to track the location of the VeriChip in real-time, but the company has been working since the chip's introduction to develop the necessary technology. The more advanced Digital Angel chip is traceable, but it is larger and worn externally in a wristwatch, rather than being implanted under the skin. The Digital Angel chip can monitor conditions such as heart rate, blood pressure, body temperature and provide tracking information. If the device notices a potential problem in the wearer, it can contact emergency medical personnel to inform them of the situation and the wearer's location. In theory, the Digital Angel chip would inform medical personnel that the wearer is about to

suffer a problem (such as a heart attack) before it actually happens. The company plans to implement those features in the VeriChip in the near future.

The problems with these chips are obvious. With tracking capabilities, the chip provides the ability to track the location of the wearer in real-time. Applied Digital Solutions claims that the chip's tracking ability is disabled, and only activated manually by the wearer, or when the chip detects an emergency. The Digital Angel, the only chip that currently provides tracking ability, is worn externally, and thus could be removed by the user if they fear being tracked. This is not possible with the skin-implanted VeriChip. Once the VeriChip achieves tracking capabilities, the wearer will have to trust that Applied Digital Solutions is not spying on them, and that the company is not providing the government with tracking equipment. Since the chips are wireless, they fall prey to all of the vulnerabilities that currently effect wireless devices, and are susceptible to interception by a third party.

In addition, the technology raises the question as to whether any government would ever make the "chipping" of its citizens mandatory. Thus far, the USG appears to prefer invasions that are external (SSNs and drivers' licenses), and we can only hope that they do not choose a more invasive measure of identification and monitoring.

There are obvious benefits to the chips, such as placing them in your children's clothing to make tracking easier in the case of a kidnapping incident, or placing them in pets' collars or under their skin to track a lost pet. One recent story extols the benefits of chips for pets: A cat with an ID microchip implanted under his skin was returned to his owner 10 years after he jumped out a window and vanished (MSNBC "Chip helps"). Modern chips that allow tracking would have enabled the family to find the pet almost immediately. Perhaps a tracking chip would have enabled authorities to find Elizabeth Smart. Balancing the safety benefits of implanted

chips with their privacy risk requires openness and information disclosure. Parents should choose external chips placed in an item such as clothing, and parents must have control over the chip's activation, operation and deactivation. In addition, parents must have handheld tracking devices that would allow them to determine their child's location instantly. When a kidnapping occurs, the parent must be able to alert authorities quickly, before the kidnapper can change the child's clothing. The externally worn chip is much less invasive than the implanted version, although each has considerable privacy risks.

Late in 2003, Applied Digital Solutions introduced a new version of their implanted chip, with improved software operating on Applied Digital Solution's servers. The new chip and supporting software would allow the wearer to connect their bank accounts and credit cards to the chip's ID number. This would enabled a chipped individual to complete a purchase at a chip-enabled POS (Point-of-Sale) device or withdraw money from a chip-enabled ATM machine by simply standing close to a chip reader attached to the POS device or ATM machine. One of the problems with this chip is that it transmits its signal by broadcast, creating the possibility that a criminal could construct a device that would capture the broadcast signal out of the air, decode it and use it in an identity theft scheme (Declan McCullagh "An ATM").

Social Engineering: Getting the Information From its Source

Miller describes social engineering as, "The attacker uses human nature to fool the victim into allowing improper access or revealing private information" (226). In many cases, the best way to gather personal information is to query the source. By nature, human beings are careless and easy to deceive, making them perfect targets to divulge their own personal information.

Site spoofing has become a very common means of tricking individuals into providing their personal information. The thief creates a page that looks exactly like a known Web page.

Creating an exact copy of a given Web page or Web site is very easy, using the "Save As" feature in Microsoft IE6. This feature allows the user to save an exact copy of the Web page currently loaded into the browser, including all of the images displayed on the page. Next, the thief registers a domain very similar to that of the page they are copying (often using common typographical errors that might occur in the address, such as adding an 's' to the end of Hotmail, or typing an 'n' instead of an 'm'). Another variation of this attack uses the @ sign in a URL to redirect the page to another location. For example, http://hotmail.com@mydomain.com would load the page located at mydomain.com, not hotmail.com. Then, the attacker uses a form on the copied page to capture data entered by unwitting users. Site spoofing is successful because the page looks exactly like the one users thought they were visiting, and most users do not pay close attention to the address of the site in the browser. According to Alorie Gilbert,

> "This rapidly proliferating form of online fraud—called—phishing—involves imposter e-mails and Web sites that look like they are from legitimate companies such as eBay. When people enter their passwords, credit-card numbers and other personal information, a thief on the other end collects the information to make charges on customer credit cards" ("Tech Firms").

Phishing has become such as prolific activity that eBay, Citibank and PayPal, the most common organizations spoofed in phishing attempts, have launched extensive campaigns to inform customers regarding eMail schemes. These companies provide information on their Web sites regarding information that they legitimately collect via eMail, and methods to prevent becoming a victim of phishing. Companies have banded together and formed the APWG (Anti-Phishing Working Group) to develop cross-industry methods of combating phishing attempts. Despite attempts to inform customers, the number of phishing messages is increasing rapidly, as

is the number of customers that suffer identity theft resulting from responding to an illegitimate message. According to Jennifer Barrett, "GIANT, an anti-spam software company, has seen more than double the number of phishing e-mails so far this month [January 2004] than in all of 2003...Citibank has already identified five fraudulent e-mails sent out to customers" ("'Phishing For'"). Although a few phishing attempts come from teenage hackers, the majority of them come from organized crime syndicated located in Europe and Asia (Barrett "'Phishing For'").

Experts have suggested a handful of technological advances to prevent spam and phishing attempts from reaching their intended recipient, although it will be at least late-2004, and realistically 2005 or 2006, before their implementation. Two of the most promising proposals have been submitted by Microsoft and Yahoo!, and each company has been trying to garner support for their respective solutions. The solutions are different, but each would require better domain authentication on the sender's eMail address before sending a message. The Anti-Spam Community Registry submitted a proposal to ICANN for a .mail gTLD (generic Top Level Domain) that would attempt to separate legitimate senders from illegitimate ones. Registering for a .mail address requires an organization to provide an extensive amount of documentation verifying its identity and purpose, along with a hefty registration fee. While this would not stop spammers from using other gTLDs for spam and phishing attempts, it would provide a "safe" gTLD for legitimate companies.

Overhearing a conversation is the best low-tech method of gathering information. For example, "Toys 'R Us" requests the customer's phone number during checkout. The sales associate, customers waiting in the same checkout line and customers in nearby checkout lines can overhear the customer's telephone number. The members of the "R" Us family (Toys 'R Us,

Babies 'R Us) seem to be particularly adept at gathering personal information. The following excerpt is from their privacy policy:

> "The "R" Us Family members collect personally identifiable information that you provide when you make a purchase; visit the Retail Stores, the Online Stores, or the "R" Us Sites; create or edit your Registries and Wish Lists; participate in a contest or sweepstakes promotion; fill out a survey or questionnaire; sign up for a survey; contact an "R" Us Family member (by e-mail or otherwise); contact "R" Us Family customer service representatives; or otherwise interact with an "R" Us Family member. Information that you provide at the Retail Stores may be combined with information that you provide online at the "R" Us Sites and Online Stores as well as with information about your product interests and purchases. The information you provide to "R" Us Family members may also be combined with demographic and other information that is publicly available in order to allow the "R" Us Family members to better communicate with you and enhance your shopping experience" (ToysRUs.com "The 'R'").

The privacy policy does not mention the company's practice of requesting customers' telephone number at checkout. Some "R" Us stores have posted a sign at the checkout counter stating that providing your telephone number is optional. Unfortunately, the stores posted signs after the company began requesting customer's telephone numbers, allowing them gather numbers for an extended period without properly informing the customer of their rights. Interestingly, the signs direct the customer to the privacy policy to find information regarding this practice, yet the privacy policy does not mention telephone numbers specifically, only personal information in general. One must question how the "R" Us stores use customers' telephone number, and the answer is simple: Some of the telemarketing calls that consumers receive probably came from

the "R" Us company's use of customer information. The following selection, taken from the same privacy policy, states the "R" Us policy on information usage (the author added the italics to emphasize two particular sentences):

> **"Using Your Personal Information** Your personal information is used by the "R" Us Family members to enhance your guest relationship with them, respond to your requests, tailor offerings to you, *communicate with you about products, services, special offerings, and events or programs offered by the "R" Us Family members or their marketing partners that may be of interest to you.* The "R" Us Family may also use this information to analyze and manage its businesses. Aggregate data (which does not allow an individual to be identified, contacted, or located) is collected from online and offline facilities and may be used to enhance the ability of the "R" Us Family members to communicate with you and for internal analysis and management purposes."
>
> "*From time to time you may receive periodic mailings, telephone calls, or e-mails from "R" Us Family members with information on new products or services, discounts, special promotions, upcoming events, or other offers from an "R" Us Family member or its marketing partners*" (ToysRUs.com "The 'R'").

The company's privacy policy plainly states that an "R" Us family member or marketing partner may contact customers regarding product offerings. Two problems regarding this statement stand out: The first is "Who are these marketing partners?" and the second is "How do these companies know for sure which offers a consumer would like informed about?" The following selection, taken from the same privacy policy, states the "R" Us policy on information sale (italics added for emphasis):

"Sharing Your Personal Information "R" Us Family members will not license, sell, or provide your personal information to any unaffiliated third party except as permitted by this policy or with your consent. The "R" Us Family shares your personal information as set forth below:

With "R" Us Family Members. *Personal information collected by one member of the "R" Us Family will be used by that member in accordance with this policy and may be shared with other "R" Us Family members for use only in accordance with this Privacy Policy...*

In Connection with Business Transfers. *In the event that a store, division, or part or all of an "R" Us Family member (or the assets of one of those entities) is bought or sold, customer information will likely be included among the transferred business assets*" (ToysRUs.com "The 'R'").

The corporation states that it will not sell information to any unaffiliated third party, except as permitted by the policy or through consent. One must wonder who defines an affiliated third party, and what steps are necessary to become an affiliated third party. In addition, the policy plainly states that if the "R" Us company sells assets that include personal information, the company will sell the customer information as part of the agreement. If the company that purchases the assets (including the customer information) has no regard for customer privacy, then expect that company to sell the customer information as often as possible.

As another example of social engineering, individuals usually do not consider the risks of cellular phone usage, and often provide information to everyone standing in a relatively close proximity. The problem worsens when the conversation occurs over a poor connection, as the cellular phone user often shouts into the phone in an attempt to make themselves clear to the

other party. The increasing ubiquity of cellular phones means that more people are using cellular phones that do not have the common sense or knowledge to use them correctly and privately. People, especially business people, need proper training and instruction on the various uses (and misuses) of cell phones (John C. Dvorak "Dangerous Phone"). After overhearing a phone conversation on an airplane, Dvorak wrote the following in a column: "The guy goes on and on. I find out his name. I find out his position. I find out he's flying to Boston in a few days. I know his schedule. I know who he works for. I'm hearing other names and extension numbers. Wow. I'm finding out far too much information" ("Dangerous Phone").

Methods of mass transportation, such as airlines, subways and busses, pose the largest threat when considering the problems of portable devices. As wireless capabilities become commonplace on airplanes, airlines are reminding passengers of the dangers posed by laptops and PDAs (Tony Hallett "Airline security"). According to Hallett, "While snooping over someone's shoulder in a plane won't allow files to be copied in the same way as an electronic breach, there are security issues. These are compounded—as with loud public mobile phone conversations—when users of a laptop or PDA in a train, bus or other public place forget they are 'out in the open'" ("Airline security").

Office and network design practices at the organizational and personal levels can also reveal plenty of private information. Many individuals have their computer monitors placed in such a way that a casual observer can read everything that is on the screen. Protective shields would prevent this, as would simply turning the monitor a different direction. Employees often leave private materials scattered around their desk or work area. Leaving the room for a moment opens up the information to the prying eyes of everyone else in the room. Many organizations label every computer and peripheral with its network name, location and IP address. While this is

an acceptable strategy from an administrative point of view, it would have been better to place the labels somewhere on the devices where they were not visible to every customer in the store. Providing customers with that information only makes it that much easier for them to hack into the local network, or for other employees to steal computing resources.

Occasionally, information release can cause great personal embarrassment, as in the case of the 19-year-old woman that accused Kobe Bryant of rape. According to an AP report, "The name of Kobe Bryant's accuser was mistakenly posted on a state court Web site Tuesday as part of a legal filing in the case. A subpoena showing the 19-year-old woman's name and address was up for about an hour before court staffers reposted it with her personal information blacked out" (MSNBC "State mistakenly"). Unfortunately, this was not the first disclosure of the woman's name, although it was the first time it was revealed by sources directly involved in the case. Bryant supporters had previously posted the woman's name on Web Sites and a radio talk show host had previously disclosed the woman's name on air.

This occurrence requires special attention, because while the accidental disclosure on the state court's Web Site was accurate, the information (including photographs) posted on many other Web Sites was not. All of the Web Sites that contained incorrect information contained the same information about another female, somehow mistakenly identified as the accuser. The spread of the information was so prevalent, and the amount of retribution the wrongly identified female suffered so great, she took her story of mistaken identity to the newspapers and airwaves in an attempt to clear her name. This is a perfect example of the dangers associate with false positives, and why it is critical that information be properly gathered, maintained, stored and verified. Inaccurate information and false positives can ruin and endanger innocent lives.

The Lurking Dangers of Identity Theft

The Information Age has made identity theft a much more serious problem then ever before. According to Lemos, "The research firm [Gartner] estimates that 3.4 percent of U.S. consumers – about 7 million adults – have been victims of identity theft of some form in the past year" ("Analyst: Crime"). According to Sullivan,

> "Nearly 10 million consumers have been victimized by some form of identity theft in the past year [2002], the Federal Trade Commission said Wednesday...Victims lost $5 billion because of the crime last year, FTC officials said, and businesses have lost close to $50 billion dealing with the problem...the FTC concluded that 27 million adults had been victimized by some form of ID theft in the past five years" ("FTC: Millions").

And now it appears that identity theft is becoming a tool of criminal syndicates. According to Sullivan,

> "Miguel Hernandez and his extended family moved into a dream, half-million-dollar hideaway home along the banks of the Columbia River in Vancouver, Wash., on April 1...the small palace was just one of 23 homes the family is said to have purchased in the past two years, scooping up $4 million worth of properties...all of them purchased by identity theft, according to local police ("Alleged ID").

Organized identity theft rings may start with individual families that plan elaborate crimes, but it is only a matter of time before organized crime begins using identity theft to carry out complex operations globally.

Credit card theft is the main threat of identity theft. Once someone has access to an individual's credit card or credit card number, they have access to their credit line, and possibly

other personal information. According to Lemos, "Gartner found that 5.5 percent of the U.S. adults surveyed, or 11 million nationally, were victims of credit card fraud" ("Analyst: Crime").

A startling and disturbing trend in identity theft cases is the rate at which identity theft is striking children. An estimated 500,000 children have their identity stolen each year (Janet Shamlian "Main culprits"). Hundreds of thousands of children are having their identity stolen each year, as loved ones, often parents or grandparents, use children's spotless credit histories for their own gains. Countless stories have surfaced already of children grown into young adulthood, only to be denied credit or employment due to a credit history that was ruined by family members. In one case, a 10-year old girl had 17 credit cards carrying thousands of dollars in balances, and had been approved for a $42,000 home loan (Shamlian "Main culprits"). All of the accounts belonged to her mother, who had opened them in her daughter's name and SSN.

The USG has unleashed a strong offensive against identity theft. A series of commercials hit the airwaves in 2003, and all 38,000 Post Offices around the country erected matching posters (Sullivan "Beware ID"). In addition, the government sent 3,000,000 information booklets to consumers across the country (Sullivan "Beware ID"). Late in 2003, Congress began considering controversial legislation to prevent identity theft. The problem with the national legislation is that it takes precedence over state legislation, which is often much stricter and provides better assurances to victims of identity theft (Sullivan "Congress mulls"). Consumer groups are against federal legislation, because it will allow credit card companies and credit bureaus to continue with their lax practices in dealing with identity theft, one of the reasons why the crime is reaching epidemic proportions (Sullivan "Congress mulls"). Unrelenting in their pursuit for privacy protection, the consumer groups intensified their efforts. According to Sullivan, "In October, The Foundation for Taxpayer and Consumer Rights, a California group, made its point

by using an airplane skywriter to write the first five digits of Citigroup CEO Charles Prince's social security number above Citigroup headquarters in New York" ("Congress mulls"). This same advocacy group posted the SSNs of Attorney General John Ashcroft and other government officials on a Web site to protest the USA PATRIOT ACT. The group's actions prove the point that information is too readily available and the government must take immediate action to prevent identity theft. Federal legislation is necessary, but it must be strict and protective of consumers.

Section Summary

This section provided a look at many emerging technology that are potential threats to individual privacy. However, since they are still emerging, the level of their threat has not reached its full potential. Given their potential for future threat, these emerging technologies raise the Privacy Threat Indicator to 4.50. If this analysis were taking place two years in the future, the discussed technologies might produce a greater change in the Privacy Level Indicator. However, diligent protests could cause many organizations to rethink their use of these technologies.

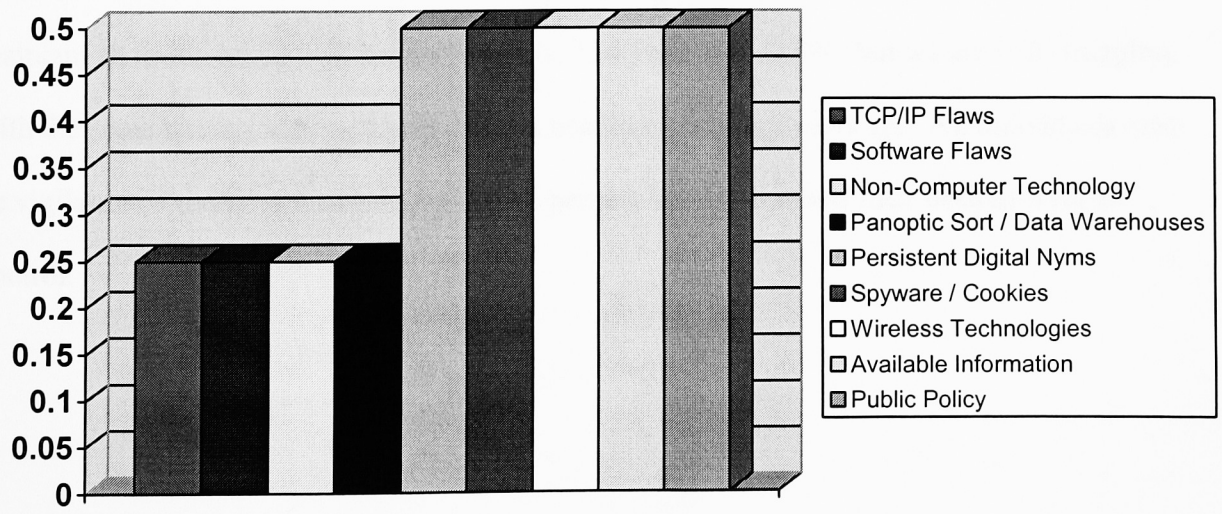
Conclusion

Conclusion

This thesis sought to answer the following hypothesis: *Changes in public policy and technological advances have greatly reduced the level of individual privacy in modern society.* Its goal was to define and measure the "privacy level", a quantifiable element describing the availability of privacy in relation to changes in current events, technology and public policy. The privacy level indicates the amount of control that individuals have over their own panoptic information, leading to "control" as the natural definition for the term privacy. Measuring

changes to the privacy level required the development of a new tool, the Privacy Level Indicator. The Privacy Level Indicator measured changes in society, technology and public policy, to determine the current privacy level, and by definition, the availability of privacy in modern society.

It was determined that the current privacy level is 4.50 – Threatened, implying that individuals concerned with keeping their panoptic information private must be vigilant in their efforts to maintain privacy, but also offering some control, while providing hope for the greater availability of privacy in the future. To cause a large increase in the Privacy Level Indicator, a threat required proof of current exploitation. A threat with a high potential for privacy invasion without proof of current usage caused a smaller change to the Indicator. In the future, any one of the factors examined in this thesis could increase their threat to individual privacy, pushing the Indicator closer to its highest level. Conversely, any of the examined factors could lower their threat to individual privacy, causing a decrease in the Indicator. The following chart details each threat's increase to the Privacy Level Indicator:



The measurements determined that the hypothesis was true, exposing a direct link between

changes in society, technology and public policy and changes in the privacy level. These changes have greatly reduced the availability of privacy in modern society.

We are dealing with a new existence, in which technology improves at an unimaginable rate, and a few terrorists can change the face of the world. Public policy must change at a rate matching changes in technology and society to assure proper privacy protection. In 1890, Samuel D. Warren and Louis D. Brandeis described a world in which technology and public policy were producing a detrimental invasion of privacy ("The Right"). Warren and Brandeis saw the need for legal protection in that era, stating,

> "That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society" ("The Right").

Even though the founding documents of our country do not provide any basis for a "right to privacy", experts have proven beyond a doubt through the years that such a right should exist to maintain an individual's well being. It may be 114 years since 1890, but we are still struggling with the same issues today as dominated the headlines so many years ago. All individuals must be vigilant in striving to maintain a personal privacy level that meets their desired level of control.

Bibliography

Albrecht, Karen. "Supermarket Cards: The Tip of the Retail Surveillance Iceberg." Denver University Law Review 79(4) (2002): 534-539, 558-565.

Anonymous. "A study of student privacy issues as Stanford University." Communications of the ACM 45 (2002): 23-25.

Barrett, Jennifer. 28 January 2004. "'Phishing' for Dollars". MSNBC (Newsweek). 28 April 2004 <http://www.msnbc.msn.com/id/4079364>.

Berlind, David. 30 June 2003. "TRUSTe issues privacy ultimatum to Batteries.com. Are you next?" ZDNet. 29 April 2004 <http://www.techupdate.com/techupdate/stories/main/0%2C14179%2C2914180%2C00.html>.

Black, Jane. 17 October 2003. "Smile, you're being watched." MSNBC (BusinessWeek Online). 28 April 2004 <http://msnbc.msn.com/id/3225985/>.

---. 5 March 2004. "Shutting Shopping Bags to Prying Eyes". BusinessWeek Online. 28 April 2004 <http://www.businessweek.com/technology/content/mar2004/tc2004035_8506_tc073.htm>.

Blumenfeld, Laura. "Dissertation could be security threat." The Washington Post. 8 July 2003: A01.

Broersma, Matthew. 24 November 2003. "Exchange flaw could open up user accounts". ZDNet. 27 April 2004 <http://zdnet.com.com/2100-1105_2-5111330.html?tag=tu.scblog.6673>.

Brostoff, Stephen. "GLB allows privacy abuse, Minn. Says." National Underwriter 106 (2002): 42.

Carlson, Caron. 11 August 2003. "Who's Minding Your Data?" eWeek. 29 April 2004

<http://www.eweek.com/article2/0,1759,1213286,00.asp>.

---. 18 November 2003. "Rights Advocates Urge Patriot Act Amendments." eWeek. 2 April 2004 <http://www.eweek.com/article2/0,1759,1387695,00.asp>.

C.A.S.P.I.A.N. "News." 8 February 2006. <http://www.nocards.org/news/index.shtml#fire>.

Cate, Fred H, and Michael E. Staten. "Does the Fair Credit Reporting Act Promote Accurate Credit Reporting?" Building Assets, Building Credit: A Symposium on Improving Financial Services in Low-Income Communities. Cambridge: Harvard University. November 18-19, 2003. Available at <http://www.msb.edu/prog/crc/JCHS%20WP%20BABC%2004-14.pdf>.

Cole, Eric. Hiding in plain Sight: Steganography and the Art of Covert Communication. New York: Wiley, 2003.

Coursey, David. 29 October 2003. "Is your car spying on you?" Anchordesk. 2 April 2004 <http://reviews-zdnet.com.com/AnchorDesk/4520-7296_16-5098423.html>.

Diffey, Larry. Letter. eWeek: The Enterprise Newsweekly 11 November 2002: 40.

Dommeyer, Curt, and Barbara Gross. (2003). "What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies." Journal of Interactive Marketing 17(2) (2003): 34-51.

Dotinga, Randy. 31 December 2002. "Biometrics Benched for Super Bowl." Wired. 16 July 2003 <http://www.wired.com/news/culture/0,1284,56878,00.html>.

Dvorak, John C. 30 June 2003. "Dangerous Phone Calls." PC Magazine. 31 July 2003. <http://www.pcmag.com/article2/0,4149,1142083,00.asp>.

Eggen, Dan. 13 December 2003. "FBI Applies New Rules to Surveillance".

The Washington Post. 30 April 2004: A01.

eWeek (Associated Press). 2 April 2004. "EU Orders Legislation on Spam, Cookies". 28 April 2004 <http://www.eweek.com/article2/0,1759,1560493,00.asp?kc=EWNKT0209KTX1K0100440>.

Fadia, Ankit. "Getting geographical information using an IP address". Astalavista Security Group. 15 July 2003 <http://www.astalavista.com/library/basics/organisation/ip-geography.shtml>.

Fisher, Dennis. 12 January 2004. "New DHS Border Plan Scrutinized". eWeek. 29 April 2004 <http://www.eweek.com/article2/0,1759,1434120,00.asp?kc=EWNKT0209KTX1K0100440>.

---. 23 February 2004. "RSA Keeps RFID Private". eWeek. 28 April 2004 <http://www.eweek.com/article2/0,1759,1536569,00.asp>.

Flanigan, Robert L. 27 June 2005. "Military Culls Student Info." Democrat and Chronicle. 27 June 2005 <http://www.democratandchronicle.com/apps/pbcs.dll/article?AID=/20050627/NEWS01/506270326/1002/NEWS>.

Fordahl, Matthew (The Associated Press). "Watching the Watchers: Anti-terrorism device is designed to dive into data at government request yet protect privacy." Democrat and Chronicle 13 July 2003: 5E.

Frenkel, James, ed. True Names and the opening of the cyberspace frontier. New York: Tor, 2001.

Garfinkel, Simson. Database Nation: The Death of Privacy in the 21st Century. Sebastopol: O'Reilly, 2000.

Garofoli, Joe. "Privacy concerns about library checkout device". San Francisco Chronicle

4 March 2004: A-20.

Giffin, John, et al. Covert Messaging Through TCP Timestamps. Proceedings of Workshop on Privacy Enhancing Technologies, 2002, San Francisco. Heidelberg: Springer-Verlag Heidelberg, 2002.

Gilbert, Alorie. 12 August 2003. "Postal ID plan creates privacy fears". CNET News.com. 17 September 2003 <http://news.com.com/2100-1028_3-5062617.html>.

Gilbert, Alorie. 2 September 2003. "Tech firms band together on ID theft." CNET News.com. 4 September 2003 <http://news.com.com/2100-1019-5070601.html>.

Gilbert, Alorie. 14 November 2003. "'Smart Shelf' test triggers fresh criticism". ZDNet (CNET News.com). 28 April 2004 <http://zdnet.com.com/2100-1103_2-5107918.html>.

Gourley, David, et al. HTTP: The Definitive Guide. Sebastopol: O'Reilly, 2002.

Goldstein, Amy. 8 September 2003. "Secrecy masks Patriot Act's conduct". The Washington Post. 30 March 2004 <http://community-2.webtv.net/Crimson_Twilight/SecrecyShroudsUSAPA/>.

Goo, Sara Kehaulini. "Fliers to Be Rated for Risk Level: New System Will Scrutinize Each Passenger, Assign Color Code". The Washington Post. 9 September 2003: A01.

---. "Airlines Hustling On Data Disclosure: Policies Being Drafted Under Pressure". The Washington Post. 24 January 2004: E01.

Greenfield, David. "Digital Identity's Hidden Maestro." Network Magazine March 2003: 40-43.

Hallett, Tony. 5 August 2003. "Airline security warns of shoulder surfing." ZDNet. 4 September 2003 <http://zdnet.com.com/2100-1105_2-5059907.html>.

O'Harrow, Robert Jr. "U.S. Backs Florida's New Counterterrorism Database." The Washington Post 6 August 2003: A01.

Howlett, Debbie. "Patriot Act battle is fought locally." USA Today 14 July 2003: 3A.

Information Awareness Office. "Human ID at a Distance (HumanID)." 16 July 2003 <http://www.darpa.mil/iao/HID.htm>.

Kanellos, Michael. 9 March 2004. "MSN Messenger flaw allows hard-drive access". ZDNet. 27 April 2004 <http://www.zdnetindia.com/techzone/resources/security/stories/99587.html>.

Keoing, David. 10 September 2003. "Shipping clerk flies in crate as air cargo". Lawrence Journal-World (MSNBC). 29 April 2004 <http://www.ljworld.com/section/archive/story/144997>.

Kerr, Jennifer C. (Associated Press). 27 August 2003. "Privacy advocates buy data on Tenet, Ashcroft". newsobserver.com. 17 September 2003 <http://newsobserver.com/24hour/technology/story/981420p-6886753c.html>.

Kewney, Guy. 23 January 2004. "RFID? They're Already Following You". eWeek. 28 April 2004 <http://www.eweek.com/article2/0,4149,1454477,00.asp>.

Kotadia, Munir. 3 December 2003. "Hijacked PCs spread 30% of spam". MSNBC (CNET News.com). 28 April 2004 <http://msnbc.msn.com/id/3660513/>.

Kravets, David. (Associated Press). 2 October 2003. "Federal appeals court declares federal DNA act unconstitutional". Casper Star Tribune. 2 April 2004 <http://www.casperstartribune.net/articles/2003/10/05/news/wyoming/05c9f0f75c00b65dab6bd530b087c4f8.txt>.

Lemos, Robert. 21 July 2003. "Analyst: Crime pays for identity thieves." 31 July 2003.

<http://news.com.com/2100-1009_3-5050295.html>.

---. 9 December 2003. "Slip-up exposes database to prying eyes." ZDNet (CNET News.com). 29 April 2004 <http://zdnet.com.com/2100-1104-5118138.html>.

Levine, John R., Ray Everett-Church, and Gregg Stebben. Internet Privacy for Dummies. New York: Wiley, 2002.

May, Timothy C. "True Nyms and Crypto Anarchy." Frenkel 33-86.

McCullagh, Declan. 25 November 2003. "At ATM card under your skin". MSNBC (CNET News.com). 29 April 2004 <http://msnbc.msn.com/id/3607047>.

McCue, Andy. 14 August 2003. "Gillette shrugs of RFID-tracking fears". eWeek. 28 April 2004 <http://zdnet.com.com/2100-1103_2-5063990.html>.

Meeks, Brock N. 12 January 2004. "TSA defends new passenger screening system." MSNBC. 27 April 2004 <http://msnbc.msn.com/id/3941260>.

Microsoft TechNet. 25 June 2003. "Microsoft Security Bulletin MS03-021: Flaw In Windows Media Player May Allow Media Library Access (819639)." 18 July 2003. <http://www.eu.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-021.asp>.

Miller, Michael. Absolute PC Security & Privacy: Defend Your Computer Against Outside Intruders. Almeda: SYBEX, 2002.

Mitchell, Shena. "The new age of direct marketing." Journal of Database Marketing & Customer Strategy Management 10 (2003): 219-229.

MSNBC (The Associated Press). 13 April 2003. "U.S. buys data on foreign citizens." 31 July 2003. <http://stacks.msnbc.com/news/899805.asp>.

MSNBC (The Associated Press). 29 May 2003. "Wanted man caught on 'Kiss

Cam.'" 31 July 2003. <http://www.msnbc.com/news/919896.asp?0cv=CB20>.

MSNBC (The Associated Press) . 5 June 2003. "Ashcroft wants Patriot Act widened." 16 July 2003 <http://stacks.msnbc.com/news/922454.asp>.

MSNBC (The Associated Press). 16 September 2003. "State mistakenly posts name of Kobe's accuser." 17 September 2003 <http://www.msnbc.com/news/967758.asp>.

MSNBC (The Associated Press). 26 September 2003. "Chip helps cat return after 10 years." 2 April 2004 <http://www.msnbc.msn.com/id/3088123/>.

MSNBC (The Associated Press). 17 October 2003. "Finns ready cellphone tracking law". 28 April 2004 <http://msnbc.msn.com/id/3226848/>.

MSNBC (Reuters). 28 October 2003. "CIA displays some of its spy gadgets". 29 April 2004 <http://www.msnbc.com/news/986186.asp?0si=->.

MSNBC (The Associated Press). 22 November 2003. "FBI collecting antiwar-group data". 30 April 2004 <http://msnbc.msn.com/id/3540810/>.

MSNBC (The Associated Press). 23 December 2003. "Airports to fingerprint, photograph foreigners". 29 April 2004 <http://www.msnbc.msn.com/id/3790183>.

MSNBC. 6 February 2004. "Brazen intruder strolls onto jet at LAX". 29 April 2004 <http://www.msnbc.msn.com/id/4191736/>.

MSNBC (The Associated Press). 17 April 2004. "Bush urges renewal of Patriot Act". 29 April 2004 <http://www.msnbc.msn.com/id/4766075>.

MSNBC (The Associated Press). 28 April 2004. "ACLU battles FBI over ISP customer data". 30 April 2004 <http://www.msnbc.msn.com/id/4856599>.

MSNBC (The Associated Press). 29 April 2004. "Lawmakers vow to pass anti-spyware

law". 30 April 2004 <http://www.msnbc.msn.com/id/4865172/>.

MSNBC (The Associated Press). 21 February 2005. "ChoicePoint to rescreen all customers". 9 March 2005 <http://msnbc.msn.com/id/7007430>.

MSNBC (The Associated Press). 9 March 2005. "Another big data broker reports breech". 9 March 2005 <http://www.msnbc.msn.com/id/7139522/>.

MSNBC (The Associated Press). 18 January 2005. "FBI abandons Carnivore wiretap software". 9 March 2005 <http://www.msnbc.msn.com/id/6841403/>.

MSNBC (Reuters). 29 November 2004. "Brain scans detect more activity in those who lie". 9 March 2005 <http://www.msnbc.msn.com/id/6609019>.

MSNBC (The Associated Press). 13 July 2004. "Ashcroft details uses of Patriot Act". 9 March 2005 <http://www.msnbc.msn.com/id/5431486>.

MSNBC (The Associated Press). 30 June 2004. "Court: E-mail providers can read Messages". 9 March 2005 <http://www.msnbc.msn.com/id/5336185>.

MSNBC (The Associated Press). 14 January 2005. "FBI holds huge cache of traveler data". 9 March 2005 <http://scj.msnbc.com/id/6828259>.

MSNBC (The Associated Press). 14 November 2004. "Trial shows how spammers operate". 12 March 2004 <http://www.msnbc.msn.com/id/6492244>.

MSNBC (The Associated Press). 21 June 2005. "CVS pulls Web service after data leak." 7 February 2006 <http://www.msnbc.msn.com/id/8305849/>.

Murray, Frank J. "NASA Plans to Read Minds at Airports." The Washington Times 17 August 2002: A01.

Mathieson, Rick. "brain storm: the truth behind nasa's top-secret mind-reading machine." 16 July 2003 <http://www.cooltown.com/mpulse/1202-nasa.asp>.

NewsRx.com. 3 May 2004. "Survey: Organizations achieving HIPAA compliance, seeing positive results." Retrieved 6 May 2004 from Proquest.

Nowak Glenn J., Joseph Phelps, and Giles D'Souza. "Antecedents and consequences of consumer privacy concerns: An empirical investigation." Journal of Interactive Marketing 15 (2003): 2-17.

Novak Glenn J., Joseph Phelps, and Elizabeth Ferrell. "Privacy concerns and consumer willingness to provide personal information." Journal of Public Policy & Marketing 19(1) (2000): 27-41.

Oldenburg, Don. "The snoop in your coupe." The Washington Post 9 September 2003: A01.

Priest, Diana. "New Spy Satellite Debated On Hill." The Washington Post 11 December 2004: A01.

Rose, Matthew and Dazhi Yang. "Keeping Information Safe: An Exploration of Teacher Practice and Perceptions in K-12 Schools." Center for Education and Research in Information Assurance and Security Tech Report 2004. Available from <https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2004-28.pdf>.

Rowland, Craig. "Covert Channels in the TCP/IP Protocol Suite." First Monday 2 (1997): Retrieved 6 May 2004 from <http://www.firstmonday.org/issues/issue2_5/rowland/index.html>.

Sanders, Aaron D. "Utilizing Simple Hacking Techniques to Teach System Security and Hacker Identification." Journal of Information Systems Education 14 (2003): 5-9.

Savage, Charles. 22 January 2004. "Infiltration of files seen as extensive: Senate panel's

GOP staff pried on Democrats." The Boston Globe. 30 March 2004 <http://www.boston.com/news/nation/articles/2004/01/22/infiltration_of_files_seen_as_extensive/>.

Scanit. "Browser Security Test Statistics." 26 April 2004 <http://bcheck.scanit.be/bcheck/sid-42634bcf592decd0c320838a6b8ed37b/stats.php>.

Shamlian, Janet. 3 March 2005. "Main culprits in kids' ID theft? Family members". MSNBC. 9 March 2005 <http://www.msnbc.msn.com/id/7045490/>.

Shankland, Stephen and Scott Ard. 4 March 2004. "Hidden text shows SCO prepped lawsuit against BofA". ZDNet. 27 April 2004 <http://zdnet.com.com/2100-1104_2-5170073.html>.

Schneier, Bruce. 30 January 2004. "Slouching toward Big Brother". CNET News.com. 30 March 2004 <http://news.com.com/2010-1028-5150325.html>.

Shelat, Abhi and Simson L. Garfinkel. "Remembrance of Data Passed: A Study of Disk Sanitization Practices." IEEE Security & Privacy 1 (2003): 17-27.

Shim, Richard and Alorie Gilbert. 9 July 2003. "Wal-Mart cancels 'smart shelf' trial". ZDNet (CNET News.com). 28 April 2004 <http://zdnet.com.com/2100-1103-1023934.html?tag=nl>.

Sipior, Janice C., Burke T. Ward and Sebastian M. Rainone. "Ethical Management of Employee E-Mail Privacy." Information Systems Management 15 (1998): 41-47.

Sullivan, Bob. 11 August 2003. "The secret tricks that spammers use". MSNBC. 29 April 2004 <http://msnbc.msn.com/id/3078640>.

---. 3 September 2003. "FTC: Millions hit by ID theft." MSNBC. 17 September 2003 <http://stacks.msnbc.com/news/960638.asp?0sl=-21>.

---. 16 September 2003. "Beware ID theft, post offices warn." MSNBC. 28 April 2004 <http://msnbc.msn.com/id/3078442/>.

---. 6 October 2003. "Alleged ID theft clan on the run". Online Security (MSNBC). 28 April 2004 <http://www.onlinesecurity.com/links/links654.php>.

---. 17 November 2003. "Congress mulls ID theft provisions". MSNBC. 29 April 2004 <http://msnbc.msn.com/id/3475290/>.

---. 8 February 2004. "Government agency exposes day-care data". MSNBC. 29 April 2004 <http://www.msnbc.msn.com/id/4186130/>.

---. 12 March 2004. "BJ's Wholesale suspects credit card leak". MSNBC. 29 April 2004 <http://msnbc.msn.com/id/4516301>.

---. 14 February 2005. "Database giant gives access to fake firms". MSNBC. 9 March 2005 <http://www.msnbc.msn.com/id/6969799/>.

---. 8 March 2005. "ChoicePoint files found riddled with errors". MSNBC. 9 March 2005 <http://www.msnbc.msn.com/id/7118767/>.

---. 24 January 2004. "Aol customer list stolen, sold to spammers". MSNBC. 12 March 2005 <http://www.msnbc.msn.com/id/5279826>.

Sunbelt Software. 13 November 2003. "Do You Archive Your Email?" 29 April 2004 <http://www.sunbelt-software.com/sunpoll.cfm?id=73>.

Teichner, Martha. 21 April 2002. "Close Watch". CBS News Sunday Morning. 30 April 2004 <http://www.cbsnews.com/stories/2002/04/19/sunday/main506739.shtml>.

The Smoking Gun. 2 September 2003. "More Sleazy 'Survivor' Secrets". 29 April 2004 <http://www.thesmokinggun.com/archive/hastiemain1.html>.

ToysRUs.com. 1 May 2002. "The 'R' Us Family Privacy Policy." 9 September 2003

<http://www.amazon.com/exec/obidos/tg/feature/-/285520/
103-0006765-7898269>.

Trigaux, Robert. "Cameras scanned fans for criminals." St. Petersburg Times 31 January 2001: <http://www.sptimes.com/News/013101/TampaBay/Cameras_scanned_fans_.shtml>.

Warren, Samuel D. and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4 (1890). Retrieved 6 May 2004 from <http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html>.

Wexelblat, Alex. "How is the NII Like a Prison?" Frenkel 99-123.

Wolverton, Troy. 19 January 2000. "AmEx, Discover forced to replace cards over security breach". CNET News.com. 29 April 2004 <http://news.com.com/2100-1017-235818.html?legacy=cnet>.

WJLA ABC News 7 (Associated Press). 7 April 2004. "ACLU Sues Government Over 'No-Fly' List". 29 April 2004 <http://www.wjla.com/news/stories/0404/137840.html>.

Yahoo! News India (Reuters). 16 November 2004. "China plans to have over 100 eyes in the sky by 2020". 9 March 2005 <http://in.news.yahoo.com/041116/137/2hwa9.html>.

Curriculum Vitae

Education

2002-Present **Rochester Institute of Technology** **Rochester, NY**

- Master of Science in Information Technology
- Telecommunications Technology, Technology Management and Electronic Commerce Concentrations
- Final Grade Point Average is 3.93/4.0

2002 **Clarion University of Pennsylvania** **Clarion, PA**

- Bachelor of Science in Information Systems
- Graduated Cum Laude

Certifications

- A+, Network+, Microsoft Certified Professional in Windows 98

Employment History

2006-Present **Xerox Global Services** **Rochester, NY**

Software Engineer

- Analyzed ASP.NET applications for SQL Injection, Cross Site Scripting, Buffer Overflows, POSTDATA Injection and other vulnerabilities using WebInspect 4.2.
- Secured Windows 2003 and Internet Information Services using Microsoft Baseline Security Analyzer and CIS Scoring Tool. Documented security processes and configuration settings to reduce errors in server deployment.
- Installation, configuration and management of three Windows 2003 Network Load Balancing clusters and one SQL Server 2005 cluster.

2005-Present **Democrat and Chronicle** **Rochester, NY**

Programmer / Analyst

- Administration of Citrix Access Suite 4.0 environment, including a twenty-two server Citrix farm and Access Gateway appliance. Currently implementing Citrix's Crystal Reports for improved farm

management. Currently evaluating the Citrix Presentation Web Server Interface for SharePoint. Administration of Wyse thin clients using NetXfer and Rapport. Experience diagnosing problems with Windows CE and ICA client configurations and upgrades.

- Administration of Windows 2003 domain controllers and one-hundred Windows 2000/2003 servers, including Windows Server Update Services. Improved Sarbanes-Oxley compliance process by creating automated Crystal Reports to obtain user and computer account information and server inventory information from Windows 2003 Active Directory and SolarWinds Engineer's Edition 8.
- Installation, configuration and management of Windows SharePoint Services for Windows 2003. Utilized SharePoint for improved productivity, collaboration and document management. Currently testing SharePoint as a viable replacement for existing Intranet portal. Extended SharePoint with the Microsoft Solutions Accelerator for Sarbanes-Oxley, which improved the automation of the internal Sarbanes-Oxley compliance process. Utilized SharePoint Configuration Analyzer for configuration verification.
- Installation, configuration and management of Automated Deployment Services for Windows 2003. Utilized ADS in conjunction with Sysprep for improved bare metal deployment of servers.
- Installation, management and scheduling of reports using Crystal Reports Server XI. Report creation using Crystal Reports Developer XI.
- Administration of network infrastructure consisting of five Cisco routers and numerous switches in a multiple VLAN environment. Utilized SolarWinds Engineer's Edition 8 and SolarWinds Orion server to monitor six T1 lines. Troubleshooting Point-to-Point WAN connections in response to service outages, bandwidth shortages and hardware failure. Configured NetFlow on routers and managed traffic flows using NetFlow Analyzer 4. Created automated Crystal Reports to analyze the information recorded by SolarWinds Engineer's Edition 8, improving the network management process.
- Currently evaluating BartPE as an altemative to Windows PE for troubleshooting and administration tasks.

- Additional experience: VMWare Workstation 5 and ESX Server 2.5, VirtualCenter 1.2; Dell/EMC CLARiiON CX300 SAN; Avocent DSView 3; SQL Server 2000 and Data Transform Services; Metabase Explorer; TreeSize; robocopy; Visio 2003

2004 **Genuine Technologies, Incorporated** **Brockport, NY**

Programmer / Network Administrator

- Designed and developed a Web-based Point-of-Sale application using PHP and mySQL. Reduced existing application code by 75%. Designed and developed the database structure. Migrated client data from a SQL Server 2000 database to a mySQL 4 database using Intelligent Converters mySQL Conversion Kit. Assisted in creating scripts to convert existing records for use in new system.
- Managed Web server availability and health statistics using cPanel, Server Monitor Professional and VisualPulse Web Edition. Managed mySQL server availability and health statistics using cPanel, Navicat, SQLyog and mySQL Administrator. Managed SQL Server 2000 health statistics using Teratrax Database Manager.
- Utilized WAPT 3.0 to create and execute scripts for load testing of production Web server. Server was tested for its ability to handle simultaneous user logons and order generations. Analyzed test results to determine server sizing and required network and user bandwidth.
- Enabled SNMP and logging on PIX firewall. Utilized Paessler Router Traffic Grapher 4.0.5 and Kiwi Syslog Daemon 7.1.4 to monitor firewall traffic, health and user behavior data.
- Utilized OpManager 5, NetScan Tools 5 and SolarWinds Engineer's Edition 7 to create network maps and scan for open ports and shares. Configured SNMP on workstations for asset management.

2000-2002 **Clarion University of Pennsylvania** **Clarion, PA**

Network Administrator

- Utilized Internet Information Services 5.0 log files and VisualRoute 6.0b to determine the identity and physical location of a hacker.
- Utilized network traffic graphs and baseline measurements to detect the existence of a server providing illegal software downloads.

- Assisted in planning and reorganizing the domain structure for the Computer Information Science department at Clarion University during migration from Windows NT 4.0 to Windows 2000 Active Directory.
- Installation, configuration, and management of Novell Netware Server versions 4.1 and 5.1. Upgraded servers from version 4.1 to version 5.1. Performed clean installations of Novell Netware Server 5.1. Configuration and administration of Novell News Server.
- Assisted professors in preparing and testing laboratory assignments.
- Taught a legally blind student about computer hardware and repair through hands-on instruction.
- Managed twenty-five student employees.
- Managed on-campus computer lab consisting of sixty Windows-based workstations. Implemented removable hard drive bays to create a "Zero Downtime Lab Environment." Created a hard drive cloning system by installing two empty removable drive bays into a computer dedicated to drive cloning. This reduced the time required to rewrite the image to a corrupted drive by one third, by enabling drive imaging on one local computer, rather than across the network. The computer dedicated to drive cloning was assembled from spare components, producing tremendous cost savings compared with the cost of professional drive duplicators.

Papers and Publications

- Sanders, Aaron D. "Public Policy and Technology: Advancing Civilization at the Expense of Individual Privacy." (Masters thesis. Rochester Institute of Technology, 2006).
- Sanders, Aaron D. "Utilizing Simple Hacking Techniques to Teach System Security and Hacker Identification." Journal of Information System Education. Volume 14, Number 1 (2003). Pages 5-9.
- Madison, Dana E. and Aaron D. Sanders. "Data Communications Concepts - Layer by Layer." 2001 Information Systems Education Conference (ISECON 2001) in Cincinnati, OH. November 2001.