Global Information Assurance Certification Paper

Privacy In A Digital Age:
Three Emerging Threats To Privacy

SANS GIAC Certification Practical Assignment
Assignment v. 1.4b Option One

Christopher Bollerer
July 28, 2003

Table Of Contents

1.0 Introduction

In July 2002, Wired Magazine published an article by Brendan I. Koerner entitled "How To Disappear." [1] Like Jonathan Swift's *A Modest Proposal*, the article is satirical yet it does provide a good overview of the issues facing everyday citizens with respect to privacy in a networked world. Among Koerner's suggestions – destroy credit cards, pay attention to privacy statements, obtain a new social security number, stop using cell phones, move, and wear a disguise at all times.

Underscoring Koerner's concerns, privacy-related headlines have begun to dominate the media, rising to the forefront of information technology-related news across both new and traditional varieties of media. The three most pervasive issues have revolved around:

- Identity theft;
- Surveillance in public areas; and
- Cookies and data mining.

The terrorist attacks of September 11, 2001 and subsequent terrorist activities have only heightened the need and call for increased measures with respect to information collection and awareness. This, in turn, has increased privacy advocates' concerns about privacy rights and the laws enacted to collect and disseminate information.

With the ever-growing importance of information technology in the world, it is not surprising that issues of privacy and identity have surfaced as prime concerns. Information technology itself is proving a mixed blessing – it has opened the doors to information capabilities many previously only dreamed about. It has, however, given many the opportunity to unfairly profit using information residing on those very same IT systems proving beneficial to so many.

Throughout the past several years, the world has been forced to open its eyes to issues of identity theft and surveillance cameras. Attempts have been made to balance an overriding concern for public safety and welfare with individual rights to privacy. These attempts have involved groups never previously involved with issues of information technology or online privacy. Groups of like-minded individuals are uniting to fight real and perceived threats. Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) [2] and the Global Internet Liberty Campaign (GILC) [3] for instance, have found followers from every corner of the globe uniting behind their concerns for privacy in various arenas. From the ACLU to metropolitan police departments, everyone's getting involved. But no clear solutions have emerged from the heated discussions taking place.

2.0 Identity Theft

---

1 *Koerner, Brendan I. "How To Dissappear" Wired Magazine, July 2002. URL: http://www.wired.com/wired/archive/10.07/start.html?pg=14 (July 2003).*

2 *Consumers Against Supermarket Privacy Invasion and Numbering. URL: http://www.nocards.org (July 2003).*

3 *The Global Internet Liberty Campaign. URL: http://www.gilc.org (July 2003).*

According to the Federal Trade Commission (FTC), one of the fastest growing types of fraud is identity theft. [4] Identity theft is the assumption of another's identity through illegal methods for fraudulent purposes.

Due to advances in technology, identity theft perpetrated against individuals or information systems no longer requires a great amount of technical knowledge or skill. Advances in technology have also allowed law enforcement officials and even consumers to identify perpetrators more easily. In addition, the increased availability of technology has allowed for the swift resolution of many issues surrounding identity theft.

Over the last few years, the rise in identity theft occurrences has skyrocketed. According to TechWeb News, identity theft rose 80% in the past year affecting 3.4% of all adult consumers. Additionally, according to Gartner analyst Avivah Litan, identity thieves face only a one in 700 chance of being apprehended.[5] Privacy-related headlines are continually dominated by issues revolving around identity theft.

There exist various methods by which criminals obtain information about their potential victims. The FTC has identified the following as some examples of how such personally identifying information is intercepted.

Identity Theft Case Study #1

In March of 2002, Florida resident Donald McNeese was charged with illegal transfer of personal information for the purposes of committing credit card fraud and money laundering. The 30-year old former Prudential employee was arrested following a 19 month investigation. McNeese was attempting to sell 60,000 names and personal information of Prudential employees at the time of his arrest.

As this example outlines, information leading to potential thefts of identity is often stolen from the institutions trusted to maintain the integrity of that information. This information is then sold for profit.

Source: Sullivan, Brian. "Florida Man Faces Charges of Identity Theft." March 7, 2002, URL: http://www.cnn.com/2002/TECH/internet/03/07/identity.thief.idg/ (July 2003).

- Criminals often obtain sensitive, personally identifying information by stealing wallets or purses containing identification, credit cards and bank cards.
- Mail, containing bank and credit card statements, credit card offers with application forms, new checks or tax information, is stolen or intercepted.
- Change of address forms are filled out by the perpetrator. This allows the diversion of mail to alternate locations.
- Criminals may obtain sensitive data, checks, account statements, credit card applications or other information by rummaging through trash.
- Credit reports may be obtained fraudulently. As these reports have a great deal of sensitive information, they can be used as a means to assume the identity of the victim.

[4] *Federal Trade Commission. URL: http://www.consumer.gov/idtheft/. (July 2003).*

[5] *Ferrell, Keith. TechWeb News. "Identity Theft Soars, But Its Still A Low-Tech Crime." URL: http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20030723/tc_cmp/12802694. (July 2003).*

- Home invasions may yield credit card or banking information, checks, identification or other personally identifying information.
- Perpetrators may pose as legitimate business people, using social engineering techniques to obtain information directly from the potential victims.
- As the volume of data on the Internet increases, so does the likelihood of exploitation of such data. Criminals may be able to gather enough information about a potential victim to perpetrate identity theft.
- Physical or virtual record theft from businesses possessing personal information may result in widespread identity theft. [6]

Identity Theft Case Study #2

For over a year, beginning in February, 2001, Juju Jiang recorded keystrokes on computers used by consumers at 14 Kinko's stores in New York. Jiang reportedly captured over 450 user names and passwords and used them to open bank and credit card accounts online. Jiang was apprehended and is currently awaiting sentencing. Similar cases have been reported, including the installation of keystroke monitoring software at Boston College.

As this case demonstrates, identity theft can involve many people and appear where least expected. Perpetrators often take advantage of institutions and public infrastructures utilized by many.

Source: Jesdanun, Anick. Associated Press, URL:http://story.news.yahoo.com/news?tmpl=story&u=/ap/20030722/ap_on_hi_te/cybercafe_security_2. (July 2003).

It is obvious from the methods outlined above that it does not always take a great amount of technical knowledge or overall skill to obtain information that may be used for the financial gain of criminals. Similarly, the ways in which criminals use this information is often very basic but very effective. [7]

- Criminals often call credit card issuers to change the mailing address of credit cards allowing the thief to charge to the stolen card without alerting the consumer.
- Stolen information is often used to open new credit card accounts. While the criminal is able to get away with large charges, it is the consumer that is left to sort out the mess.
- Phone or wireless accounts may be opened in the consumers' names.
- Bank accounts may be opened in the consumers' names and the criminal will then be able to write bad checks.
- Loans are frequently taken out in the name of the consumer. This allows the criminal to purchase big-ticket items.

In 1999, the Financial Modernization Act, also known as the "Gramm-Leach-Bliley Act" or GLB act, was introduced. The GLB Act includes various provisions to protect consumers' personal financial information held by financial institutions. The GLB Act accomplishes this in three parts:

- The **Financial Privacy Rule** is applicable to financial institutions including lenders, brokers, consumer loan services, monetary transfer services, tax preparers, financial advisers, credit counselors, and real estate agents and delineates Federal requirements for privacy of personally identifiable information.

6 *"ID Theft: When Bad Things Happen To Your Good Name." URL: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm. (July 2003).*

7 *"ID Theft: When Bad Things Happen To Your Good Name." URL: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm. (July 2003).*

- The **Safeguards Rule** is enforced by the FTC and requires financial institutions to have security plans in place to guarantee the confidentiality and integrity of personal consumer information.

- **Preexisting Provisions** include financial information protection regulations and guidance already in place. [8]

It is clear that identity theft is a growing area of concern for consumers, law enforcement officials and lawmakers. As the amount of personally identifiable information collected by the federal, state and local governments and the corporate sector grows, so does the overall threat to individuals. The information needed to perpetuate identity theft can be found in highly secure databases or in neighborhood garbage cans. Therefore, efforts to target identity theft must continue to focus on both technical and non-technical issues.

8 *"Gramm-Leach-Bliley Act, November 1, 1999." URL: http://banking.senate.gov/conf/confrpt.htm. (July 2003).*

3.0 Surveillance

Throughout the past several decades, as cameras and other types of monitoring devices have become commonplace in elevators, on street corners and in automated teller machines, Americans have been forced to accept a certain level of surveillance. There is, however, a heightened awareness of surveillance techniques that has surfaced since the terrorist attacks of September 11, 2001. In addition, the rapid development of monitoring technology, the decreasing price of that technology, and legislation passed since the terrorist attacks, have perpetuated this growth.

One concern among the American public is the use of cameras in metropolitan areas. Unlike the United States, many of the world's major metropolitan areas have employed surveillance cameras and other equipment for years. London, for example, installed cameras in order to direct emergency services and scan for terrorists and suspicious activities. The city has encountered little opposition. Within the United States, however, the idea of monitoring the public is met with hostility. Most recently, the city of Virginia Beach, Virginia proposed the introduction of a surveillance system. While funding is approved, the system is not yet in place because of opposition.

A second and perhaps more contentious issue involves the use of "red light cameras" used by many jurisdictions to capture images of vehicles running red lights. Images of both the driver and the license place are typically captured when the violation occurs. While few argue with the overall value of stopping people from running red lights, the cameras themselves have few supporters. Many see it as an invasion of privacy while others view it only as a money-making opportunity for local municipalities. In addition, the camera systems are often installed and monitored by third parties, leading to concern about personally identifiable information and its availability beyond the scope of law enforcement personnel.

Surveillance in the Marketplace

- *In 2002, AT&T began offering a service whereby wireless subscribers could locate one another, taking advantage of global positioning. Since its introduction, the AT&T service has found few interested consumers.*
- *General Motors' OnStar program – a service that offers a wide array of services from providing directions to sending help in the case of an emergency – has become a thriving business over the past three years.*
- *The niche market of surveillance equipment tailored to parents has experienced meteoric growth over the past few years. Parents have begun taking advantage of day care facilities with cameras in order to monitor their children throughout the day. Consumer electronics stores have also received an increase in business, attracting parents who wish to, with or without their children's knowledge, monitor their activities at home through cameras, or on the road, through global tracking systems.*

The marketplace reflects mixed reactions on the part of consumers.
In response to the growing use of surveillance cameras, many groups have made efforts to raise the awareness of surveillance cameras to the public. One such group is the NYC Surveillance Camera Project . Made up of members of the New York Civil Liberties Union, the group claims to have mapped every surveillance camera monitoring

the public in Manhattan. 2,397 cameras have been identified. The group offers maps and routes to avoid cameras in the area and allows users to submit camera locations. [9]

The Electronic Privacy Information Center (EPIC) has also begun working towards a greater public awareness of public surveillance. EPIC, founded in 1994 as a public interest research center in Washington, D.C., recently launched the Observing Surveillance Project in order to document the increasing presence of surveillance cameras placed in Washington DC since September 11, 2001. The overall goal of this project is to spark public debate over surveillance in public places and increase the awareness of these systems, in part through online exhibits. In addition, the group has published a database, similar to the NYC Surveillance Camera Project, informing tourists of camera locations. The project's site can be reached at www.observingsurveillance.org.[10]

As terrorism continues to pose a threat to public infrastructures around the world, it is clear that there is no easy solution to public surveillance. Legislation, and the legal tests of such legislation, will, most likely, form the standards for surveillance.

9 *NYC Surveillance Camera Project. URL: http://www.mediaeater.com/cameras. (July 2003).*

10 *Observing Surveillance. URL: http://www.observingsurveillance.org. (July 2003).*

4.0 Cookies and Data Mining

As technology has developed, so have ways of monitoring our behavior online. Many methods are employed on the Internet to collect information that, taken alone or combined with other available information, may compromise individual privacy. The use of cookies and data mining are two hotly debated methods of data collection.

Cookies were designed to allow Web sites or servers to deliver information to a client and store that information locally. In addition, cookies allow information to be returned to Web sites. This information exists in the form of small data elements stored on the clients' hard drives. These small pieces of code allow Web sits to maintain and display specific user information. As the HTTP protocol is an inherently stateless protocol, cookies allow user-specific information to be displayed without the server having to store HTTP transaction-specific information. Cookies are passive and collect no data from users' hard drives. There exist two types of cookies:

- **Session cookies** are designed to last as long as the HTTP session or until the Web browser is closed. These cookies are strictly temporary.
- **Persistent cookies** are designed to exist on the user's hard drive beyond the length of a user's Web browsing session. In fact, these cookies generally exist until erased by the user.[11]

While cookies represent passive data gathering techniques, data mining demonstrates an aggressive effort to identify patterns and establish relationships in data mined from many sources. The primary focus of data mining with respect to overall privacy concerns is information gathered from the Internet and other information systems. SearchCRM.com lists several data mining techniques often employed:

- **Association** looks for patterns where one event is connected to another event;
- **Sequence or path analysis** looks for patterns where one event leads to another later event;
- **Classification** looks for new patterns;
- **Clustering** finds and visually documents groups of facts not previously known; and
- **Forecasting** discovers patterns in data that can lead to reasonable predictions about the future. [12]

Web mining is the aspect of data mining specific to the Internet. SearchCRM defines Web mining as "the integration of information gathered by traditional data mining methodologies and techniques with information gathered over the World Wide Web."

There are many suggested ways individuals can protect their privacy online. In addition, legislation has been enacted to further protect consumers and Internet users.

---

11 *SearchCRM. URL: http://SearchCRM.com. (July 2003).*

12 *SearchCRM. URL: http://SearchCRM.com. (July 2003).*

The Children's Internet Protection Act (CIPA)

CIPA aims to protect children against obscene or inappropriate Web content by requiring Internet filters to be installed on computers in libraries that receive federal funding. [13] Typically, Internet filters screen the delivery of content based on keywords within the HTML coding of Web sites. CIPA, opposed by the ACLU and other civil liberties groups who claim it infringes on free speech, was upheld by the Supreme Court in June of 2003. [14]

Carnivore

The FBI Internet monitoring system "Carnivore" was discovered in July of 2000. Since then it has been the subject of much criticism and debate. Carnivore is an application installed at Internet Service Provider (ISP) facilities that monitors Internet traffic for delivery to monitors. Information transferred from the ISPs must be specifically classified and authorized by the FBI, however the terms of that characterization have never been released to the public. [15] Many privacy advocacy groups and concerned citizens have voiced their opposition to the Carnivore program. EPIC, for instance, filed an injunction against the FBI barring it from using the Carnivore program until it could review the program based on documentation available under the Freedom of Information Act (FOIA) .[16]

13 *Children's Internet Protection Act. URL: http://www.ifea.net/cipa.html. (July 2003).*

14 *EPIC. URL: http://www.epic.org/free_speech/cipa.html. (July 2003).*

15 *Federal Bureau of Investigation. URL: http://www.fbi.gov/hq/lab/carnivore/carnivore.htm. (July 2003).*

16 *EPIC. URL: http://www.epic.org/privacy/carnivore/complaint.pdf. (July 2003).*

5.0 September 11 and its Legacy to Privacy

The terrorist acts of September 11, 2001 raised many privacy-related issues that have been directly addressed by legislation recently enacted. Overall awareness of the dangers posed by information technology systems has increased as well as an overall increase in funding for IT security programs in the public and private sectors. Many of these changes have direct impacts on privacy policies and practices. Two examples of such impacts are the Total Information Awareness program and the PATRIOT Act.

Terrorism Information Awareness (TIA)

Formerly known as Total Information Awareness, Terrorism Information Awareness (TIA) was created by the Defense Advances Research Agency (DARPA) Information Awareness Office. The goal of TIA is to capture "information signatures" of individuals in order to track potential terrorists and criminals. These information signatures are compiled by gathering as much information as possible through the use of computer algorithms and human analysis. Data mining techniques would then be employed to sort through the compiled evidence and discern patterns and associations. [17]

Privacy advocates have long been concerned about TIA and its privacy implications. While it is a powerful tool, it could be used against those not guilty of crimes. In addition, the resulting database in which these information signatures are stored including financial, medical, communication and travel records may open innocent individuals to scrutiny. If compromised, such information may also be used by criminals with malicious intent.

The PATRIOT Act

Signed into law on October 26, 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, commonly referred to as the PATRIOT Act introduced wide-ranging legislative changes by increasing the surveillance and investigative powers of law enforcement agencies. Many privacy-oriented groups including the ACLU and EPIC observed that the act did not adequately provide a system of checks for ensuring that civil liberties were protected.

The Patriot Act effectively created or modified the following:

- Wiretap Statute (Title III)
- Electronic Communications Privacy Act
- Computer Fraud and Abuse Act
- Foreign Intelligence Surveillance Act
- Family Education Rights and Privacy Act
- Pen Register and Trap and Trace Statute
- Money Laundering Act
- Immigration and Nationality Act
- Money Laundering Control Act
- Bank Secrecy Act

[17] *Defense Advances Research Agency. URL: http://www.darpa.mil/iao/TIASystems.htm. (July 2003).*

- Right to Financial Privacy Act
- Fair Credit Reporting Act [18]

Much of the legislation stemming from the fight against terrorism is subject to challenges from civil rights groups and privacy advocates. Many consider it reactionary and seek a balance between protection of the country and individual privacy rights. Only time will tell how this balance will be achieved.

[18] *American Civil Liberties Union. URL: http://www.aclu.org/Files/OpenFile.cfm?id=12250. (July 2003).*

6.0 Conclusion

Through identity theft, surveillance, cookies and data mining, the threats to personal privacy we face on a daily basis are increasing. As technology and experience grow, so do both the threat to personal privacy and the damage that can be perpetrated. If recent trends continue, identity theft cases will continue to increase, the use of surveillance will become commonplace and data mining techniques will become increasingly more effective. Therefore, the awareness of personal privacy issues must be increased.

Both the Y2K preparation and September 11 terrorist attack fueled privacy and overall IT security issues but such efforts must continue despite the fact that threats may not be perceived as imminent.

7.0 References

American Civil Liberties Union. *URL: http://www.aclu.org. (July 2003).*

Children's Internet Protection Act. *URL: http://www.ifea.net/cipa.html*. (July 2003).

Consumers Against Supermarket Privacy Invasion and Numbering. *URL: http://www.nocards.org (July 2003).*

Defense Advances Research Agency. *URL: http://www.darpa.mil. (July 2003).*

EPIC. *URL: http://www.epic.org. (July 2003).*

Federal Bureau of Investigation. *URL: http://www.fbi.gov. (July 2003).*

Federal Trade Commission. URL: http://www.ftc.gov. (July 2003).

Ferrell, Keith. TechWeb News. "Identity Theft Soars, But Its Still A Low-Tech Crime." URL: http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20030723/tc_cmp/12802694. (July 2003).

Global Internet Liberty Campaign. URL: http://www.gilc.org (July 2003).

"Gramm-Leach-Bliley Act, November 1, 1999." *URL: http://banking.senate.gov/conf/confrpt.htm. (July 2003).*

"ID Theft: When Bad Things Happen To Your Good Name." *URL: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm. (July 2003).*

Jesdanun, Anick. Associated Press, *URL:http://story.news.yahoo.com/news?tmpl=story&u=/ap/20030722/ap_on_hi_te/cyber cafe_security_2. (July 2003).*

Koerner, Brendan I. "How To Dissappear" Wired Magazine, July 2002. *URL: http://www.wired.com/wired/archive/10.07/start.html?pg=14 (July 2003).*

NYC Surveillance Camera Project. *URL: http://www.mediaeater.com/cameras. (July 2003).*

Observing Surveillance. *URL: http://www.observingsurveillance.org. (July 2003).*

SearchCRM. *URL: http://SearchCRM.com. (July 2003).*

Sullivan, Brian. "Florida Man Faces Charges of Identity Theft." March 7, 2002, URL*: http://www.cnn.com/2002/TECH/internet/03/07/identity.thief.idg/ (July 2003).*