A Study Involving

Personal Information

and the INF Ph.D. Students

Of the School of Information Science and Policy

At the State University of New York at Albany

By

Mark C. Scott

Submitted in partial fulfillment

of the seminar requirement for

the M.L.S. degree

at

The State University of New York at Albany

ISP 680 Seminar: Information Science and Policy

December 13, 1999

Table of Contents

Abstract

In today's society personal privacy is being lost or abused by a wide assortment of organizations from mailing lists and credit card companies to World Wide Web sites. Throughout the media there are stories about people losing their identity due to a vast amount of information that is available to the public. Americans have lost the ability to control their own personal information. Research has shown that Ph.D. students in Information Science at the University at Albany have an excellent understanding of personal information and are knowledgeable in protecting their personal information. Results have shown that all Ph.D. students surveyed have requested that their personal information not be shared with other companies. This study also found that 87.5% of the students have purchased products on the Internet, and that they followed precautions to ensure that their personal information was protected while online. It was also found that more than half of the students were concerned about providing personal information to obtain a credit/debit card.

Introduction

As the new millennium approaches massive changes are taking place with computer technology, and an individual's ability to obtain different types of information. Today people can use their computers to find directions to a small town in southern Utah or see the firsthand results of global warming. A 1992 opinion survey found that "79% of Americans believe that computers have improved the quality of life yet the same survey found that 68% of Americans agreed that computers were a threat to personal privacy."[1] Statistics such as these coincide with Louis D. Brandeis and Samuel D. Warren's warning, "Numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops."[2] Alderman and Kennedy, authors of *The Right to Privacy*, note that the computer is the device that outstripped all other threats to privacy.[3]

Besides being able to locate information, computers also store and manipulate more than ever before. Though computers are able to perform numerous, critical advanced tasks, everyone must be aware of the dangers to privacy that can be created and revealed with a computer. With advances in computer technology, information on a given individual can be acquired and in some cases even altered with a single keystroke. The large-scale use of computers and databases has produced major concerns over the issue of privacy. Computer databases now store more information for longer periods of time. The kinds of information that are stored have a wide range from credit reports to a person's favorite brand of toothpaste.

This research focused on four areas that are essential in examining the subject of information privacy: the uses and abuses of Social Security numbers, privacy issues concerning the credit card business, the Internet and e-commerce, and data lists.

The School of Information Science and Policy

The researcher surveyed the students in the Information Science Doctoral Program at the School of Information Science and Policy at the State University of New York at Albany. The Nelson A. Rockefeller College of Public Affairs and Policy administers this degree. The program is designed to prepare graduates for careers in academics or research in information science centering on information management or governmental positions in policy or the private sector. The major components that must be completed to graduate include:

- Four interdisciplinary core proseminars
- Research tool and information technology competencies
- Primary and secondary areas of specialization
- Areas of specialization:
- Expert systems
- Geographic information systems
- Group decision support modeling
- Information decision systems
- Organization of knowledge records
- Public information policy
- Doctoral dissertation.[4]

The doctoral program enrolled its first group of students in 1990-91. This program combines the efforts of many departments such as the School of Business, the Department of Communication, Geography and Planning, Computer Science of the College of Arts and Sciences, the School of Information Science and Policy, and the Department of Public Administration and Policy of the Graduate School of Public Affairs. As of the fall of 1999 there were 40 doctoral students enrolled in the program. [5]

Purpose of the Study

The objective of this study was to determine by means of a survey the level of awareness and personal attitudes toward information privacy among students seeking their Ph.D. in the Information Science program at the School of Information Science and Policy at the University at Albany. The survey gathered empirical information about the students' control, use, and knowledge concerning information privacy.

Hypotheses

It was hypothesized that this collection of data on privacy would reflect the students' attitude toward current practices and issues with regard to information privacy in the late twentieth century. The researcher expected that the Ph.D. students would have strong opinions on the topics discussed in the survey. It was also believed that this particular group of students, studying all facets of information science, would have an excellent understanding of information privacy and the important issues involved. It was believed that because of the students' experiences as individuals in a technological society as well as their knowledge of the subject matter they would be concerned about

information privacy, expressing reluctance to share, or care in sharing of personal information with private and public sector organizations.

Limitations of the Study

Population Difficulties

The population of Ph.D. students consisted of (37) individuals. The problems in conducting this survey stemmed from the fact that the group was a very small population. With a small population one runs the risk of not receiving enough surveys in order to conduct the data analysis. Many of the students do not meet in a traditional class setting. Much of the course work is conducted on an individual basis. In order to issue the survey to each student the survey needed to be mailed or distributed in the 702 course. There was also the possibility that not all students who were currently enrolled in the program were available to complete the survey. Some students were on sabbatical in which case they could not be reached.

Size of the Sample

When conducting any type of survey, the party issuing the survey runs the risk of having a low return rate from the participants. It was hoped that since the survey dealt with information privacy that the students seeking their Ph.D. degrees in Information Science would be willing to taking the time to complete the survey. The sample size of this study was 16 out of the 37 students.

Anonymity

Since this was a survey on privacy none of the questions asked entailed any personal identifying information. There were however questions of a personal nature such

as the number of credit/debit card owned or the number of people in one's family. Nonetheless, the researcher had no way of knowing the identity of the respondents.

Funding and Time

The researcher was limited to the fall 1999 semester for data collection. If there had been more time the researcher could have expanded the population of the survey to include all students enrolled in the School of Information Science and Policy. The funding was limited to supplies, which consisted of stamps for postage and envelopes to mail the surveys. The researcher funded the projected.

What is privacy?

Since the inception of the Constitution the issue of privacy, in its many complex forms, has been an important issue Americans have struggled to define and maintain in this country. With the growth of computer technology, privacy is becoming more difficult to achieve. In the past before computers, personal information about individuals was public but such information was secure because everything was recorded on paper. Acquiring information could take time and such documentation could be easily destroyed.[6] Today personal information is often stored on computers in the form of databases. Information can be stored in multiple databases and is susceptible to improper use by an unlimited number of people. A complex idea such as privacy can have a broad spectrum in terms of the different forms it can take on. In many areas of life, from simply being left alone to the information individuals possess or create about themselves, privacy is a right. To understand privacy and privacy issues one must have a clear understanding of what privacy is, and the various privacy types.

Types of Privacy

A general definition of privacy can be seen as the ability to remain or keep information secluded from another individual, a larger group or organization. In his chapter entitled "Privacy: Philosophical dimensions of the literature" Ferdinand Schoeman defined privacy in three ways. First, privacy can be regarded as a claim, entitlement, or right of an individual to determine what information about him or her may be communicated to others. Next privacy can be seen in terms of the control individuals have over information on themselves, personal identity, or who has access to information on individuals. Finally, privacy can be defined as a state or condition of limited access to a person.[7] Stefano Scoglio looked at privacy in a similar manner yet he placed his concepts in terms of capitalism and its effect on privacy. Scoglio divided privacy into four different areas. The first is *physical privacy*, which concentrates on property in terms of one's home and body. The second type is *decisional privacy*, which focuses on ones ability to make decisions and choices concerning physical actions. The next type of privacy is *formational privacy*, which deals with activities such as advertising and mass culture, where penetrating the mind is the goal. The final type of privacy is *informational privacy*, which deals with the control one has of his own personal information as well as the knowledge others have on an individual. [8]

Informational Privacy

Informational privacy is often based on the issues of economics such as purchasing goods with a credit card, opening a bank account, or applying for a mortgage or loan.[9] Informational privacy also relates to specific knowledge individuals possess about themselves whether it is medical records, Social Security numbers or other actions

taken throughout a given day. The researcher was primarily concerned with issues regarding this type of privacy.

Social Security numbers

Since the 1960s the use of the Social Security number as a personal identifier has raised many debates. Some proponents believe using the number as an identifier enables better, more efficient record keeping systems. Other opposing views center on the creation of numerous and intrusive databases, and the ease with which information can be linked.[10] In the 1990s the Social Security number and its uses continue to come under attack from many privacy advocates. Discussion of the uses and abuses of the numbers has been a topic that has received much attention in Congress in recent years.

The Once Key Identifier

Today an individual's Social Security number plays more of a role than just tracking ones Social Security benefits, which the number, by law, was originally intended to do.[11] In the 1990s the Social Security number has more uses than when it was first issued. The number is becoming a less relevant identifier due to the emergence of databases and use of other linking agents such as name, address, and phone number. The rise in database technology differs from the past thirty years when the Social Security number was used as the primary identifier. Today it is easily possible to merge individuals' records without the use of the number as it is with it.[12] Yet there are still numerous areas of peoples' lives that can be accessed with this number. Universities, driver's licenses, and financial institutions all have been known to use Social Security numbers to identify individuals. It is the numerous databases and abuse of Social Security

numbers that has many people throughout the country concerned about the widespread use of this number as an identifier.

Abuses of the Social Security number

Georgetown University

There are instances recorded throughout the country in the past few years where the number is asked for and a clear reason is not provided, or the number is abused or stolen from a database. In the March 1995 edition of *Privacy Journal*, Lisa Eckstein reported on Georgetown University's questionable use of Social Security numbers. The University was sending questionnaires to parents asking for personal information on fund raising efforts. Within the survey there was a questions asking for personal information including Social Security numbers. The cards were then to be returned to the registrar's office. Eckstein, citing *The Chronicle of Higher Education*, stated that "what appears to be the registrar's office . . . is really the development office."[13] The University discontinued the survey to avoid further problems. The numbers could have been used to figure out a person's occupation, income, and property ownership. A Georgetown spokesperson eventually commented on the situation citing that the numbers make it easier to cross-reference parents who may also be alumni.[14]

Social Security Numbers and Driver's Licenses

Although the situation with Georgetown University did not result in any wrong doing there are times when the numbers are abused. In October of 1996 Congress discussed the use of Social Security numbers on drivers' licenses throughout the nation. Many states were not in favor of placing the number on licenses. The Commonwealth of

Massachusetts is aware of the threat to a person's identity that could result from such use. Massachusetts suggests drivers have the DMV use random numbers to avoid a loss of privacy if a license should be lost or stolen. Other states like Oregon have seen the problems of collecting Social Security numbers. In the summer of 1996 an individual acquired a list of driver addresses and vehicle ID numbers and posted the list on the Internet. Though the Social Security numbers were not listed there is a great fear of losing control of one's private life when situations such as this occur.[15]

Congressional action

A clear danger that can result from the misuse of the Social Security number is the theft of ones identity. Senator Dianne Feinstein (D) from California was surprised at the short amount of time her staff needed to locate information about her from a commercial database. Senator Charles Grassley (R) from Iowa believed with a small amount of information and a few keystrokes, a lifetime of personal information can be obtained.

On April 16, 1997 Grassley introduced the Personal Information Privacy Act (S.600) to the first session of the 105th Congress. This bill "amended the Fair Credit Reporting Act to redefine the term 'consumer report' to exclude identifying information listed in a local telephone directory (thereby ensuring that the personal identification information in the credit headers accompanying credit reports of unlisted individuals remains confidential)." [16] The bill also amended "part A (General Provisions) of title XI of the Social Security Act to prohibit the commercial acquisition or distribution of an individual's Social Security number (or any derivative of it) as well as its use as a personal identification number without the individual's written consent."[17] This proposal

was intended to make sure personal information could not be retrieved by unknown people with wrong intentions.[18] As of the writing of this paper there was no floor action on this particular bill.[19] The misuse of the Social Security number can result in great damage, much of which is centered around credit cards and credit history.

Credit Cards

Although the creation of credit cards has made life easier in terms of purchasing goods and services, privacy advocates believe that credit cards have caused significant problems concerning a person's privacy. As of 1994 over 80% of American households had at least one credit card and this country as a whole was charging more than $200 billion a year.[20] H. Jeff Smith notes in his book *Managing Privacy* that one in every ten dollars spent by American customers is charged on almost 300 million cards in circulation.[21] In the United States today, there are three major credit bureaus: Equifax, Inc., Experain, or formally TRW, and Trans Union Corporation. These three companies maintain information on more than 90% of the American adult population.[22] The information that such companies hold on an individual commonly includes "name, Social Security number, address, telephone number; financial status and employment information, credit history, outstanding debts, and public record information."[23]

Micromarketing

Many companies throughout the country profit from the massive amount of records credit bureaus store on individuals. Today credit card agencies use their databases to sell their information to meet the product needs of individuals.[24] Businesses are shunning old marketing techniques like advertising on television and in newspapers in

favor of using information from such sources. This new concept has come to be known as "micromarketing." Micromarketing enables companies to "know something about each consumer before deciding which ones to target."[25] By looking at what a person purchases on credit, credit card companies like American Express have created categories ranking a person's spending patterns.[26] A particular individual is now a target for companies who are looking for specific people with certain interests and likes. Enormous amounts of money can be made from those selling such information to those who are using the information.[27]

Abuses of credit cards

Major problems have occurred in terms of the abuse of personal information relating to credit cards. There have been people who have taken advantage of others' personal information such as name and Social Security number to obtain credit cards. Social Security numbers are a powerful set of digits that when used improperly can cause serious damage. An example of such misuse occurred at Modesto Junior College in California. An instructor took students' names and Social Security numbers from a class list and created fraudulent credit card accounts in the students' names. The individual behind the scheme was caught when the credit card companies began inquiring as to why the new cardholders were not paying their bills. Unfortunately the victims of this crime suffered in trying to persuade the major credit bureaus to remove this damaging information from their accounts. Credit card companies in the U.S. hold incredible power in terms of information stored on a given individual. By having access to such information an individual's personal life can be altered resulting in the abuse of their identity.[28]

Other types of abuse

There are other areas of the credit card industry where personal information can be acquired. In his book on privacy issues, Jeffrey Rothfeder proved how easy it is to acquire a person's credit report. The author interviewed a former FBI agent who knew the right databases and passwords to produce the author's credit report. Once a credit report is accessed the amount of critical information available is unbelievable. Information such as bank account numbers, and Social Security numbers, as well as credit history can be obtained. Rothefeder noted that acquiring passwords and other important numbers is not difficult. Passwords and numbers can often be obtained for a certain price. Besides paying for such information Rothefeder explained that many banks often share important information about each other's computer systems, enabling ease of entry. It is also possible to use a modem to call into a bank's Automatic Teller Machine network and access personal accounts. With the technology improving, acquiring information is becoming quite easy.[29]

Alleviating the credit card problem

Credit card companies like Visa International Inc. are working on ways to protect a person's card if it should be lost or stolen. In 1995, $1.3 billion was the total combined losses from fraudulent or counterfeit credit cards according to HNC Software Inc.[30] A 1996 article from *Information Week* stated that Visa was working on a crime stopping system called Card-holder Risk Information Service (CRIS) to protect against fraud. The software that runs CRIS "learns to recognize spending patterns of cardholders and ranks transactions according to different pattern variables."[31] As example of how CRIS works, if a cardholder exhibits regular purchases at the grocery store and gas station and

unexpectedly purchases from a jewelry store in London, CRIS sends an electronic notice to the Visa member's bank and the bank contacts the cardholder. The system has worked well for member banks. Chase Manhattan Bank, has found CRIS to be effective in preventing fraud.[32]

Data Lists

A final area that can cause difficulties in securing a person's privacy is the amount of personal information stored in data lists and databases. Data lists are similar to databases and mailing lists in that important personal information such as a person's name, and personal profile are stored. Direct marketing companies' computers are used for solicitation purposes to meet what corporate America deems an individuals' desired needs. In a 1995 Equifax/Harris Consumer Survey 80% of Americans agreed that "consumers have lost all control in how personal information about them is calculated and used by computers."[33] It appears Americans are concerned about privacy yet people constantly complain about junk mail and telephone solicitations from various companies. When phone calls interrupt family time and junk mail appears in the mailboxes, people who feel their privacy is being abused should ask to be removed from such lists. People say they care about privacy but they do not want to take the time or effort to take the necessary steps needed to eliminate such abuse of privacy.[34]

Targeting

With a society based on computer technology, Americans witness the results of technology and the role data lists play every day through telephone solicitations and junk mail. There are more than 10,000 lists of data on individuals available for purchase.[35] For

corporate America this is a brilliant tactic to keep consumers satisfied with what is available in the market place. Transactions of all types are recorded and placed on various lists for future use. If an individual uses a credit card to "purchase outdoor furniture soon brochures hawking barbecue grills, [and] lawn seed" are likely to appear in the individual's mailbox.[36] A person invites others companies to target interests and desires in purchasing related products. Completing routine tasks such as purchasing outdoor furniture or changing an address, filling out a warranty card, or applying for a mortgage can land a person on a list. This tactic of targeting is similar to micromarketing yet those controlling the lists have taken a person's information one step further by combining other list. By using targeting it is possible to pinpoint a person in terms of lifestyle, general demographics and future purchases.[37] Micromarketing just focuses on an individual's specific interests, rather than the entire person.

Magazine subscriptions

Not only are lists created on individuals and their purchasing habits but the magazines the individual subscribes to can also be an excellent targeting source because the magazine's content can be a very revealing. Carole Lane, author of *Naked in Cyberspace*, believes that if an individual receives any magazine it is very definite that the person's name is being sold on a mailing list. The publishers create a sketch of their subscribers based on percentages such as men versus women, median age, and average income. Lane sites an excellent example in her book, saying that nearly all the subscribers to *Black Enterprise Magazine* are probably African-American. Furthermore, the publisher is aware of the number of males who subscribe, and their age. In having such information the readers of the magazine are targets for specific products associated

with the magazine. Another list that can be created from magazine subscriptions is a new mover list. In notifying a magazine of a new address a person is pinpointing himself, added to a list for goods and services affiliated with the new community.[38]

Controlling the situation

As noted in the section on credit cards, those controlling the data lists purchase and sell information on a regular basis. The sale of personal information has become a multimillion-dollar operation controlled by the three leading credit bureaus.[39] It is simple to obtain personal information on a given individual from person's income to records on credit limit. People encounter some problems in being placed on these lists. Often a person loses access to and control of his information.[40] The person also does not know if his information is being used in some way. Some privacy advocates are of the opinion that a person may not be able to control the exchange of information on lists but he can control where his name appears. By not giving away personal information in such forms as entering sweepstakes, answering warranty cards and applying for shoppers club cards a person may stand a better chance in where his information goes. An individual will never be able to completely remove himself from all lists but it is possible to gain some control of personal information.[41]

Some people are taking matters into their own hands in preventing their personal information from being abused. As reported in a 1995 article in *Privacy Journal*, a California resident, Bob Arkow, developed a few methods to prevent telephone solicitation. "When ordering products or services he included a telemarketing agreement forbidding the company to call him or give out his unlisted phone number."[42] Once the company endorsed his check the company entered an agreement with Arkow whereby his

time and information was available for $500 per call. The stipulation for this amount was created by Termination Customer Provided Access (TCPA). Another tactic Arkow used when receiving a telephone solicitation was to ask if the company would remove his name from their list as well as requesting a copy of the company's do-not-call policy. By asking for the policy it required the company to lose time in sending it when other calls could be made. If 10% of people followed this tactic it would create a problem beyond repair for the companies placing the calls.[43]

Privacy and the Internet

The Internet is a global phenomenon that is changing the shape of society. At one time information was only accessible through books. Today the Internet is responsible for an incredible amount of information, which is now only a few keystrokes away. With this technology a person can purchase clothing from the L.L. Bean Web site, or access the on-line catalogue at Stanford University's Cecil H. Green Library as well as acquire personal information such as telephone numbers and maps to homes on practically any individual. Privacy on the Internet is a very complex and involved process. Purchasing products with a credit card through a well-known reliable company is a safe transaction due to encryption. As for the numerous services, databases, and information a person can provide about himself on the Internet the necessary precautions taken in everyday society must be maintained in order to ensure a certain amount of privacy in cyberspace.

E-Commerce and encryption

Today purchasing goods over the Internet is a multi-billion dollar business. Many people are turning to this new purchasing power because of the convenience and time

saving capacity e-commerce provides. However many people are hesitant to participate in this revolutionary process of shopping and purchasing products due to the privacy issues involved in providing a credit card number over the Internet.

Encryption is the method of scrambling an e-mail message or file of information so it appears unreadable to anyone who does not know how to unscramble the message. This process enables anything that is encrypted to be virtually inaccessible to anyone other than the designated recipient. In terms of purchasing goods, encryption protects financial transactions online. Only the parties involved in a transaction know who is buying or selling, what the product is and how much it costs.[44] Two leading experts, Georgetown University computer scientist, Dorothy Denning and William Baugh Jr. believe the current encryption applications cannot be decoded. As they see it "at 128 bits, finding an encryption key by exhaustively checking all possibilities is not even feasible in a lifetime using all the computers in the world."[45] Encryption enables people to feel safe and confident about using credit cards to purchase products online yet there are other areas of the Internet that may prove harmful in protecting one's privacy.

Surfing the World Wide Web

The World Wide Web receives the most attention of any facet connected to the Internet. The Web can be a valuable resource for almost any subject imaginable if the page is providing accurate information. This new resource of information is similar to the numerous databases that store information on individuals. Web sites have the ability to capture valuable information on users visiting a site such as an e-mail address, the computer model, operating system, and location of the computer. With such capabilities

the many Web pages have received negative publicity in terms of dealing with privacy issues.

Besides being able to acquire such information the Web is also full of databases that provide phone numbers, street addresses, and detail maps for a particular individual. It is also possible to purchase information from various Web sites with accounts of a person's financial information. Another questionable tactic that Web sites employ is the use of electronic devices called "cookies." These devices allow the Web site to trace the tastes and choices of consumers who visit a particular site. Such information allows companies to target advertising but also to sell this information to other companies, which creates more profiles on individuals.[46] Fortunately an individual can monitor and even delete the number of cookies that are sent to his computer.

Protection while surfing

The issue of privacy and surfing the Internet has raised many concerns for people who are frightened about the lack of privacy online. There have been occurrences where individuals have not used the proper discretion when discussing personal subjects online. Karen Coyle, a regional director of Computer Professionals for Social Responsibility in California, uses the term "Usenet droppings" whereby correspondence over the Internet can be seen by other users.[47] Coyle recalled a situation in which a woman was in a health care newsgroup complaining about her current medical plan and physician. The woman later received an e-mail from her Health Maintenance Organization (HMO) asking if she wanted to discuss her problems. The woman's HMO monitored newsgroups looking for its name and responded to comments.[48]

A 1997 Business Week/Harris poll found that 53% of Americans who responded believe laws should be passed that state how personal information can be collected and used on the Internet. Such an out lash has raised speculation concerning the federal government's role in the Internet. The Federal Trade Commission (FTC) issued a report stating that many Web sites are taking the necessary precautions to protect peoples' privacy online.[49] The Commerce Department released a report after the FTC recommended that Web sites disclose when information about a user is being collected and state what is being done with the data. The Commerce Department also mentioned that Internet users should also be able to determine how information is used and that companies who violate privacy policies will be held responsible. [50]

Ways to protect

The Clinton administration has not done much to advance privacy online. The administration has been relying on the industry to monitor itself in order to protect privacy. In surfing a numerous number of popular Web sites there is almost always a link describing the company's privacy practices. These links highlight subjects such as cookies and what is done with personal information. An individual should make a habit of reading the privacy statements and only soliciting sites which provide such information.

There are other ways to insure privacy online. An organization called the World Wide Web Consortium has created a system called Platform for Privacy Preferences. This system helps Web sites disclose privacy policies so consumers can decide what types of personal information can be given in return for goods and services. The federal government also maintains www.consumer.gov whereby people can learn how to

preserve their privacy, prevent companies from using credit records for marketing purposes, and removing names from direct marketing mailing and telephone lists.[51]

The Public and Private Sectors

A final issue that receives a large amount of discussion within the United States is the difference in how the public and private sectors of society approach the privacy question. In order to understand this debate between the two sectors one must have a better understanding of who represents each sector. The public sector relates to the government and the needs of the people while the private sector centers on corporations and profit- oriented tasks. This particular area of the privacy debate creates a very interesting situation due to the contradictory nature of politics and the economic well-being of the nation. In order for society to be successful corporate America must be functioning effectively. Companies need to reach their customers and in doing so may abuse peoples' privacy. The government needs companies to be successful but also believes that an individual is entitled to freedom of privacy.

The Debate

Ever since the first settlers came to this country the issue of privacy has been well represented in both the legal and political realms as a basic right granted to all. Unfortunately the founding fathers never included the word "privacy" in the Constitution which has lead to an ongoing debate on the issue and will continue well in to the future. One of the main problems that arise is that the federal government takes a contradictory approach to privacy. An excellent example of this approach is the Video Privacy Protection Bill better known as the Bork Bill. In 1987, a weekly Washington D.C.

newspaper published a list of videos Robert H. Bork, then a nominee for the United States Supreme Court, had rented. People were astonished that such information was available. The Act disallowed retailers from selling or revealing video rental records without concept or a legal order.[52]

This issue appeared as a threat to lawmakers, who quickly moved to pass legislation against such abuse. The debate raised however has some legislators feeling sympathetic and believing that certain steps taken for privacy can hurt the U.S. commercial trade. Lawmakers have acknowledged that within the private sector there is not a true right to privacy but rather a trade-off between a person's rights to privacy and a well-run economy. Such a situation creates an ambiguity; corporate America pushes the issue as far as possible until privacy issues arise, whereby the companies must react to alleviate the problem. In turn privacy advocates continue to push their agenda with little concern for the nation's economy. Legislators are left in the middle of the debate trying to please their constituents on both sides of the issue. [53]

Self Regulation

In order to deal with this ambiguous situation, many including the Commerce Department believe that companies who collect information must regulate themselves and each other. This type of policy can be seen first hand when visiting Web pages and reading the privacy policy. The company explains its approach on personal information, leaving the individual a choice. "Customers can choose those providers whose policies are compatible with their preferences."[54] To insure that a company's Web site abides by the privacy standards a seal of approval would be issued, and privacy trustees would monitor the site. There would also be different seals allowing the customer to decide

which he trusts more. As of 1998 there were two companies issuing seals, TRUSTe, and the Better Business Bureau. Corporations caught violating self-regulation would be subject to legal actions.[55] With self-regulation and monitors corporations can police each other to ensure an individual's privacy is not being abused.

Research Methodology

The Survey

The first step involved in preparing the survey was to devise the survey document for the piloting. (See Appendix A.) This was done with the input and assistance of Professor Deborah Lines Andersen of the School of Information Science and Policy. The survey was divided into three areas. The first section asked about credit cards and the Internet and consisted of eight questions. The second section dealt with data lists. The final section was entitled "Questions About You." This section was designed to ask questions about the students without violating their privacy. The survey included questions on the following subject areas:

- The personal information used to acquire credit/debit cards (section 1, questions 1-3)
- Concerns about purchasing goods over the Internet (section 1, questions 4-8)
- The purchasing and selling of one's personal information by companies throughout the country (section 2, questions 1-4)
- Thoughts on placing personal information into society (section 2, questions 5-8)
- Precautions taken when dealing with their own Social Security number (section 2, question 9)
- Questions on the subjects, such as age, country of citizenship, employment status, etc. (section 3, questions 1-10)

The Pilot Survey

The pilot was conducted on October 4th 1999. Professor Andersen issued the pilot survey to her research methods class at the School of Information Science and Policy. Thirty-two students participated in the survey. The students were asked to keep track of the amount of time needed to complete the survey. The allotted time was originally set for 10 minutes. After looking over each survey and the time kept, it took on average about 18 minutes to finish the survey.

The students also provided helpful insights such as commenting on the length of the survey and the amount of writing required to answer many of the questions. The students also posed some interesting viewpoints concerning the nature of the survey. For example the following quotation had appeared at the beginning of the pilot survey "You go through life dropping little bits of data about yourself everywhere. Following right after are big vacuum cleaners sucking them up. (Evan Hendricks, editor of the *Privacy Times.*")[56] Many students thought the quotation was biased, and the quotation was removed.

There were also suggestions to allow for blank spaces to answer questions rather than providing scales. After reviewing the pilot and discussing the results with Professor Andersen changes were made to shorten the survey by removing scales, placing blank spaces, and inserting directions to skip certain questions that may not have applied to certain people.

Once the survey was refined it was submitted to the University's Institutional Review Board. A panel reviewed the survey, approved the content, and determined that

the human subjects involved were not at any risk. The survey was granted approval on November 1, 1999. (See Appendix B.)

Data Collection

The time frame for this survey was limited to the last two weeks in November 1999. The survey was issued to the students in two different ways. First the survey was sent by mail on November 15th 1999 to 26 students who were not currently taking the Pro Seminar, INF 702. The survey was issued on November 17th 1999, to eleven students currently taking the INF 702 class. The surveys were completed on the student's own time and returned to Professor Bloniarz. Professor Bloniarz placed the surveys in an envelope in the School of Information Science and Policy office. The students who received their survey in the mail were directed to return the survey to the School of Information Science and Policy office by December 1st 1999.

Survey results

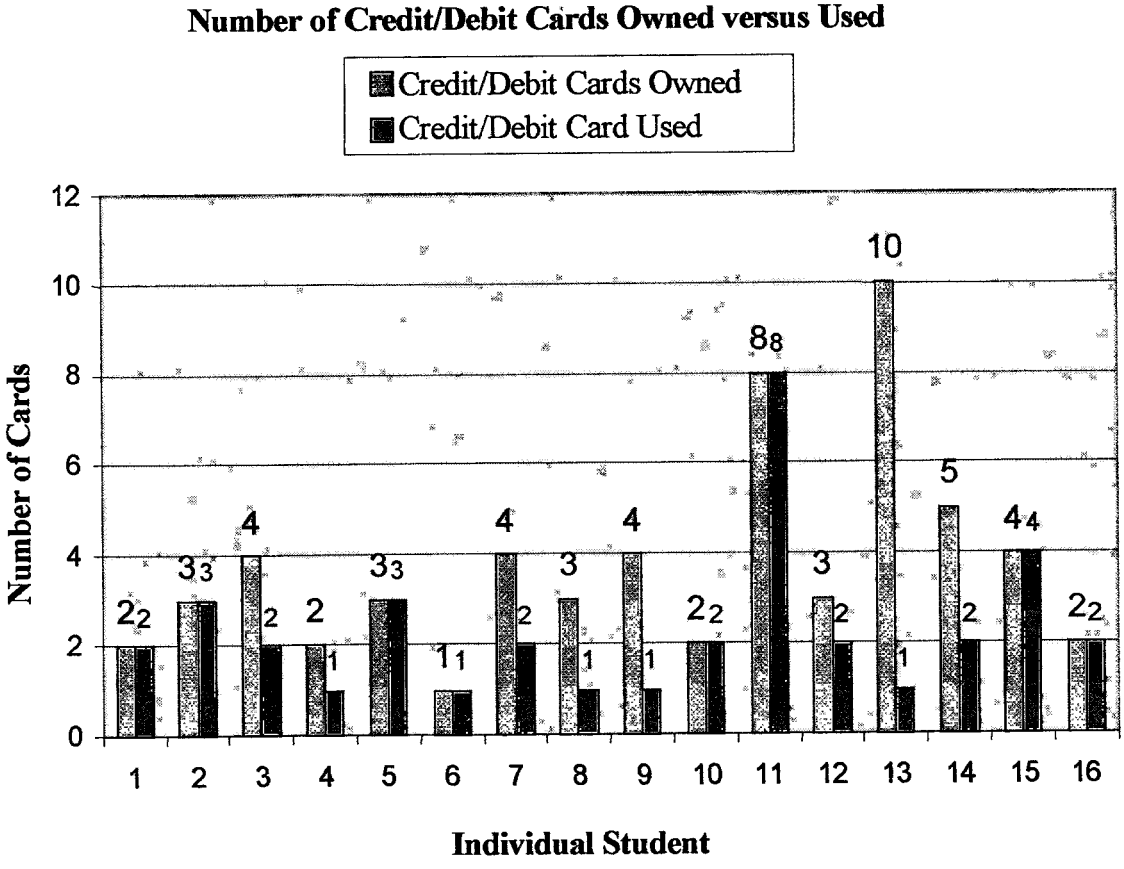
General Overview

There were 37 Ph.D. students available to take part in the survey. Of the 37 surveys, 16 or 43.24% were returned to the researcher as of December 1st 1999. Of the 37 students, 11 students received the survey in INF 702. Out of these 11 surveys, 5 or 45.45% were returned to the researcher. The other 26 students who were not currently enrolled in INF 702 received the survey by mail. Of the 26 surveys with return postage paid for, 11 or 42.30% were returned to the researcher.

Credit cards and the Internet

All 16 students who complete the survey answered questions one and two, which dealt with the number of credit/debit cards owned and used. Table 1 details the respondents and the number of cards owned versus used. The maximum number of cards owned was 10 while the minimum was 1. The mean number of cards owned was 3.75. Of the credit/debit cards being used the maximum number was 8, while the minimum was 1. The mean for credit/debit cards used was 2.31.

Table 1: (Questions 1 and 2)



The third question from the section on Credit Cards and the Internet asked if there were any concerns in providing personal information to obtain a card. Table 2 exhibits the students' responses. Nine of the 16 students or 56.25% responded "Yes" to being concerned about providing personal information. One student mentioned how he did not like giving his Social Security Number due to cross-matching techniques. While student did not feel comfortable providing such information and many felt safer keeping more personal information undeclared.

Table 2: (Question 3)

Concerns about providing personal information to obtain credit/debit cards

Response	Number of students	Percentage
Yes	9	56.25
No	7	43.75

The next question asked the students if they had ever purchased products over the Internet. The results from this question are found in Table 3. Of the 16 students to respond, 14 or 87.5% responded "Yes" to purchasing products online, 12.5% or 2 students responded "No." The fifth question was designed for those that responded "No," asking why he or she had not purchased products online. Both students stated that they would rather see and touch the product right away rather than waiting for the product. One of the two students one also expressed not wanting to send his card number over the Internet.

Table 3: (Question 4)

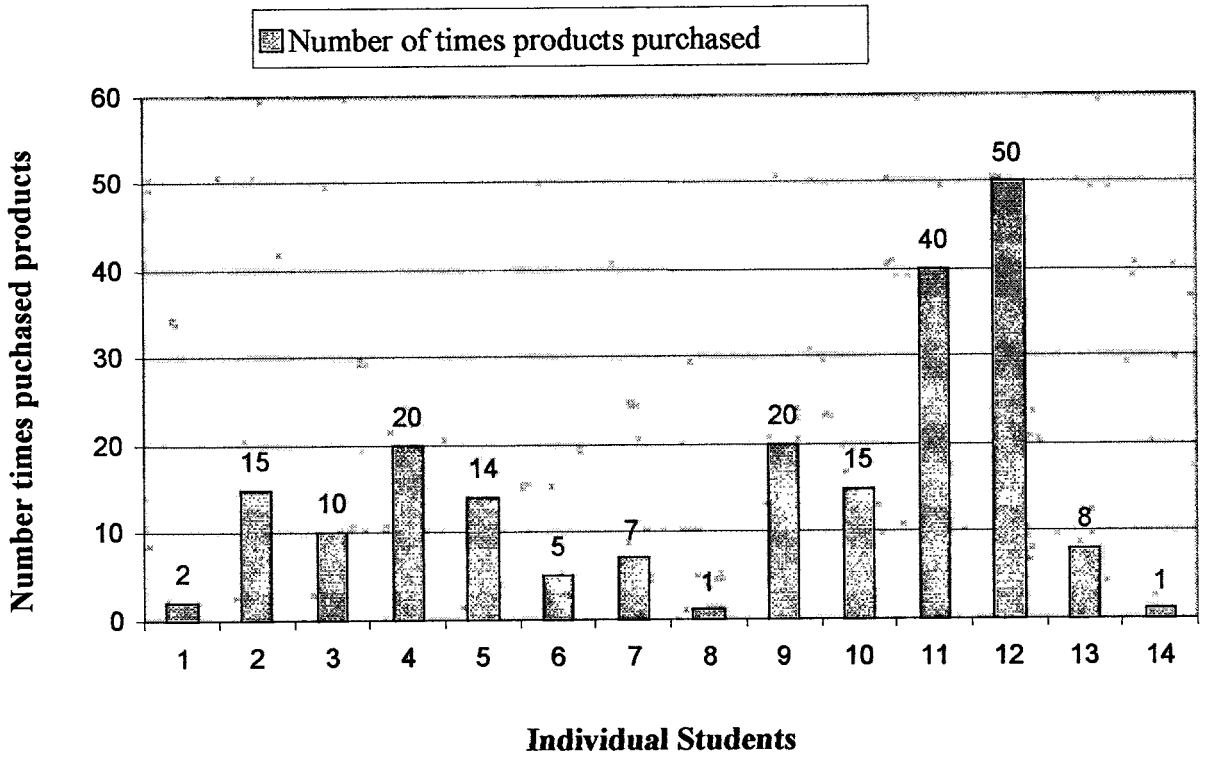
Number of students who have purchased products online

Response	Number of students	Percentage
Yes	14	87.5
No	2	12.5

Questions six through eight of this section were created for those students who responded "Yes" to purchasing products online. Table 4 details the results of this question. The sixth question asked the number of times each student had purchased products over the Internet. The mean response for the 14 student who purchased products online was 14.85 times, while the maximum number of times was 50.

Table 4: (Question 6)

Number of times students purchased products on the Internet



Question seven asked the students if there were any concerns about providing personal information over the World Wide Web. A detailed look at these responses can be found in Table 5. Eight of the 16 students or 50% responded "Yes," while 37.5% or 6 students answered "No." Both the "Yes" and "No" respondents believed that secure sites

and encryption where two key elements that must adhered to in order to purchase products online.

Table 5: (Question 7)

Concerns about providing information over the World Wide Web

Response	Number of students	Percentage
Yes	8	50
No	6	37.5
No response	2	12.5

The final question asked if the students took any precautions in online purchasing and if so what precautions. The responses to this question are in Table 6. Eleven or 68.75% of the 16 students responded "Yes," while 3 or 18.75% answered "No." Those that responded "Yes" cited precautions such as only purchasing from well-known, reputable companies, using a secure server, reading privacy statements, and only using sites that have either the Better Business Bureau or TRUSTe Logo.

Table 6: (Question 8)

Precautions take when purchasing products over the Internet

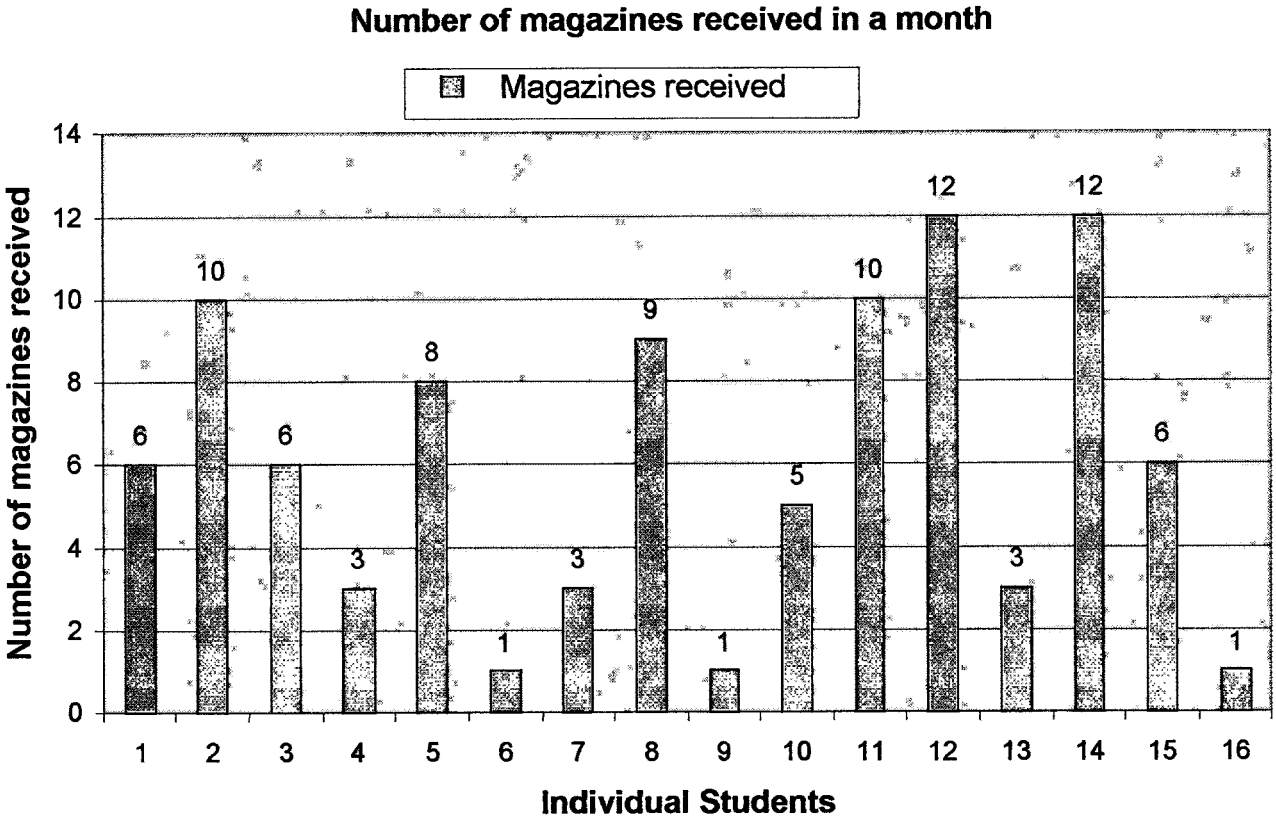
Response	Number of Students	Percentage
Yes	11	68.75
No	3	18.75
No response	2	12.5

Data Lists

The next portion of the survey focused on data lists, or information compiled on numerous individuals focusing on a person's specific interests. Many of these lists are created using magazine, catalogs, or information obtained from credit cards activity. The first question in this section asked the students the number of magazines or journals the

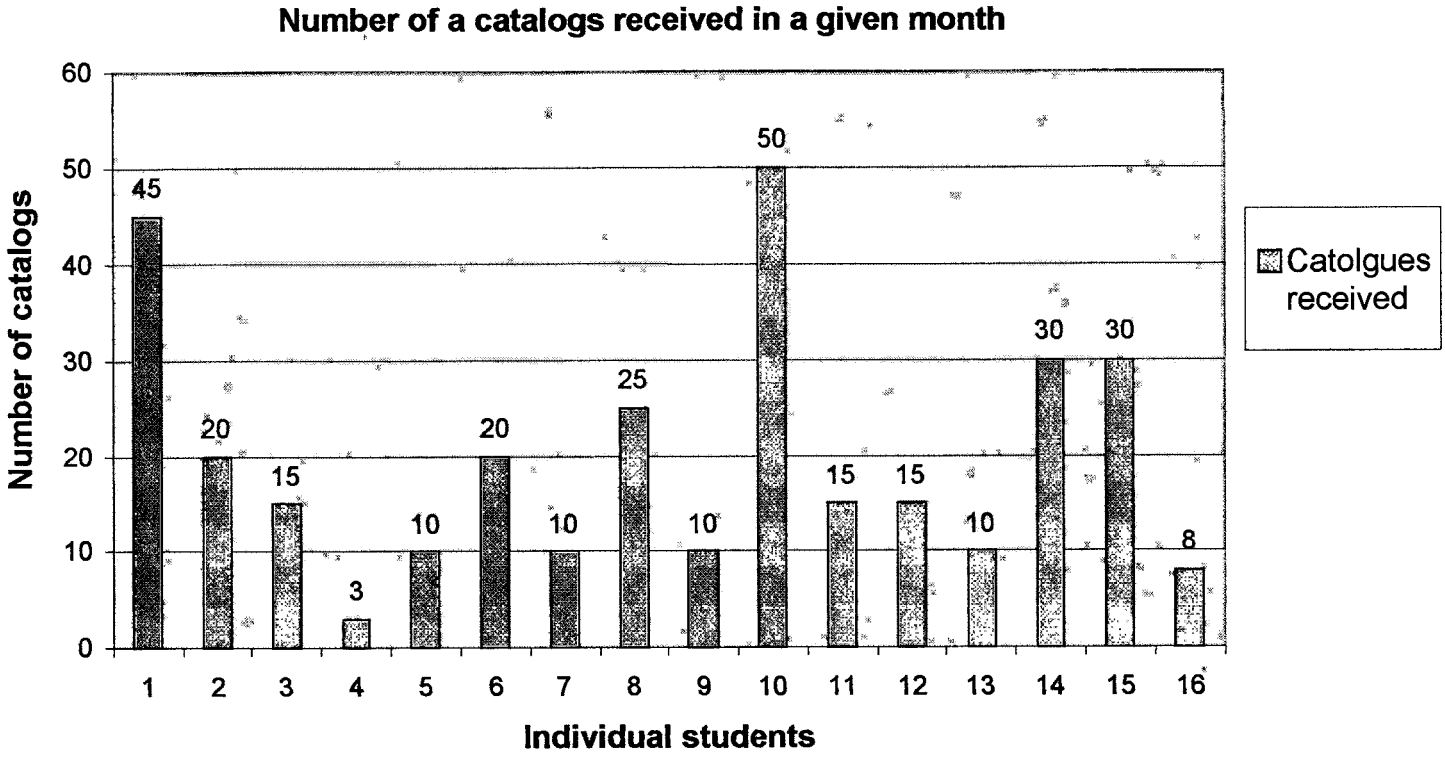
household they live in receives in the mail in a given month. Responses to this question are detailed in Table 7. The mean number of magazines received in a given month was 6, while the maximum was 12 and the minimum was 1.

Table 7: (Question 1)



The second question asked how many catalogs a household received in a given month. Table 8, exhibits the responses to this question. The maximum number of catalogs was 50, the minimum was 3, and the mean was 20.

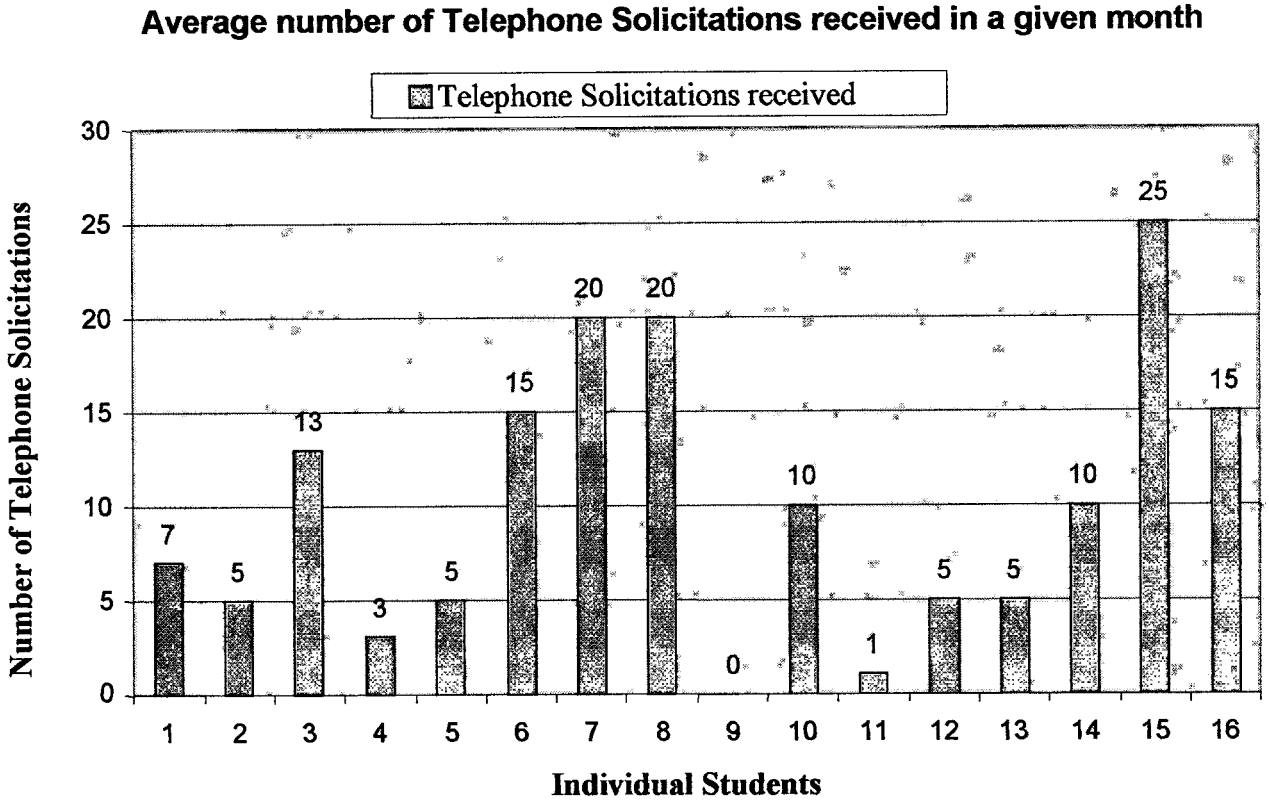
Table 8: (Question 2)



The next question asked on average the number of telephone solicitations the individual received in a given month. Replies to both the third and fourth question appear in Table 9. The minimum number of telephone solicitations was 0 calls per month, while the maximum was 25. The mean response to this question was 10 telephone calls per month. The fourth question expanded on the previous question asking the students if they had ever asked to be removed from a solicitor's list and the ease of being removed. Of the 16 students surveyed, 11 or 68.75% responded "Yes" to being removed from lists. There was a space provided for comments as to why the student wanted to be removed. An overwhelming majority of the students commented that such calls were annoying and that they did not want to be bothered. Four out of 5 students

who responded to the ease of being removed said they had no problem. The one person who had difficulty in being removed had to write a letter in order for the telephone calls to stop.

Table 9: (Question 3)



(Question 4)

Removal from Telephone Solicitation list

Response	Number of students	Percentage
Yes	11	68.75
No	5	31.25

Question five in this section of the survey asked how the students felt about their personal information being bought and sold. Table 10 shows a detailed look at this question. Twenty-five percent or 12 of the 16 students surveyed responded negatively

toward this question. The most common reply of half those surveyed was that they "Don't like it." Of the students that did not reply negatively to this question, some believed that "at times it was ok" if the information was not specific in nature.

Table 10: (Question 5)

Attitude toward companies purchasing and selling of personal information

Response	Number of students	Percentage
Positive	2	12.5
Negative	12	75
No response	2	12.5

The next question asked if the student had ever requested that a company not share their personal information. The responses to question six can be found in Table 11. An area for comments was also provided. Of the 16 students surveyed all 16 responded "Yes" to this question. Of the few who provided comments to this question, "checking the opt out box" when providing personal information was a reoccurring response. One woman concerned about her home address and directions to her home on the Internet had her family's information removed from several people's finder Web sites.

Table 11: (Question 6)

Request that a company not share personal information with other companies

Response	Number of students	Percentage
Yes	16	100
No	0	0

The seventh question was intended to find out if providing personal information had ever been helpful to any of the students. The results to this question are provided in Table 12. Eight of the 16 students or 50% of the students surveyed, said "No," they believed providing such information was not helpful to them. Thirty-one point twenty-

five percent or 5 of the 16 surveyed did however, feel that in some cases providing information was helpful. One student was able to receive information on products, especially magazines, which he might not have known about.

Table 12: (Question7)

Has sharing personal information ever been helpful

Response	Number of students	Percentage
Yes	5	31.25
No	8	50
No response	3	18.75

The eighth question asked the students to provide examples from their experiences or conversations in life that have lead them to deal differently with personal information. The results can be found in Table 13. Of the 16 students surveyed 14 answered this question. Eight of the 16 or 50% said "Yes," they had experiences or conversations that changed how they conduct their lives. Three of the 8 students mentioned classes taken within the Ph.D. program that have changed how they deal with personal information. One woman discussed how she had her wallet stolen with her checkbook and all but one credit card. She now keeps such items separate in order to avoid having her identity stolen. A student from a foreign country, stated that privacy is highly regarded in his country and there are laws that protect personal information.

Table 13: (Question 8)

Have there been experience that have led you to deal differently with personal information

Response	Number of students	Percentage
Yes	8	50
No	6	37.5
No response	2	12.5

The final question in this section asked if the students take any precautions in giving out their Social Security number and to provide any experience where their number may have been abused. The results of this question are found in Table 14. Seven of the 16 students surveyed or 43.75% said they had never had a situation where their Social Security number was abused. Seven of the 16 students said they try to avoid giving the number out unless it absolutely essential. These five students gave out their number if they know who is using the number and for what purpose, such as for medical reasons. A women said she knew of a situation where access to a Social Security number led to criminal use of information in falsify credit card applications.

Table 14: (Question 9)

Precautions taken when giving out Social Security number

Response	Number of students	Percentage
Avoid giving it out, unless essential	7	43.75
No	7	43.75
No response	2	12.5

Questions About You

This section was designed to obtain a general overview of the sample involved. This section dealt with questions on the individual such as age, gender, number of children in the home, and employment status. The first question in this section asked for the students' age. A group of age ranges was provided so the student would feel comfortable in answering the question. Table 15 shows the breakdown of the students and their ages. Seven of the 16 or 43.75% of the students surveyed were in the 40-49 age bracket. Out of the 16 students surveyed, two responded to this question with "No Way" and "Over 21."

Table 15: (Question 1)

The age range that best describes you

Age range	Number of students	Percentage
20-29	1	6.25
30-39	4	25
40-49	7	43.75
50-59	1	6.25
60+	0	0
No response	1	12.25

The second question in this section asked the students to identify their gender. The results of this question are located in Table 16. Of the 16 students surveyed 9 or 56.25% were male and 7 or 43.75% were female.

Table 16: (Question 2)

Gender	Number of students	Percentage
Male	9	56.25
Female	7	43.75

The next question asked the students to identify their marital status. The results to this question are found in Table 17. There were three choices to choose from: single, married, and divorced. Eighty-one point twenty-five percent of the 16 surveys returned or 13 students, selected the married category. Three of the 16 or 18.75% chose the single category. It was determined that all the male respondents were married and 4 of the 7 female respondents were married as well.

Table 17: (Question 3)

Marital Status

Status	Number of Students	Percentage
Single	3	18.75
Married	13	81.25
Divorced	0	0

The next set of questions focused on whether any of the students had children living in their home and if the did what were the children's ages. A detailed look at both questions four and five can be found in Table 18. Question four which asked if the students had children living in their home, yielded a 62.5% or 10 students to respond "Yes," while 37.5% or 6 students answered "No." The next question was designed for those who responded "Yes" to question four. Of the ten who responded "Yes" there was a grand total of 17 children among the respondents. Among five of the respondents, there were a total of 7 children in the 0-8 age range. Three respondents had children in both the 9-12 and 13-19 age range while two respondents each had one child in the 13-19 age range living in their home. Of the 10 students surveyed with children, none had children in the 20-25 age range living in their home. It was hypothesized that there would be some correlation between the number of children and items received in the mail. There were no systematic difference found when comparing the number of children and the number of magazines, catalogs, or telephone solicitations received.

Table 18: (Question 4)

Children living in household

Response	Number of students	Percentage
Yes	10	62.5
No	6	37.5

(Question 5)

Number of children per student in household according to age range

Age Range	Number of children per student										Total
0-8	1	1			1	2	2				7
9-12			2	1				1			4
13-19			2	1				1	1	1	6
20-25											0
Total	1	1	4	2	1	2	2	2	1	1	17

The Ph.D. program has many international students working toward their Ph.D. degrees. A breakdown of this question is exhibited in Table 20. The sixth question was intended to determine the students' country of citizenship. Of the 16 students who took part in the survey 11 or 68.75% indicated their country of citizenship was the United States. One responded was from Norway, another from Korea and two students did not answer this question.

Table 20: (Question 6)

Country of citizenship

Country	Number of students	Percentage
United States	11	68.75
Norway	1	6.25
Korea	1	6.25
No Response	2	12.5

The seventh question asked the students to select from a list of nine areas dealing with specific requirements and courses to be completed in order to earn one's Ph.D. The question was intended to see how far each student was into the program. Table 21 gives a detailed view of the students and the areas they had completed. Of the 16 students surveyed 13 or 81.25% responded to this question. Twenty-five percent of the students had completed INF 701. All but one student surveyed had not completed this course. Of the 13 students to respond the average number of the nine subject areas completed was 5.49. While only 3 students had completed their proposal defense and only one student had defended his dissertation.

Table 21: (Question 7)

Courses Completed

Requirement	Number of students to complete	Percentage complete
701	12	75
702	11	68.75
703	10	62.5
704	11	68.75
Comprehensive Examination	10	62.5
Major specialization qualifier	6	37.5
Minor specialization qualifier	5	31.25
Proposal defense	3	18.75
Dissertation defense	1	6.25
No response	3 students	

The eighth through tenth questions in this section asked the students about their employment, what they currently did, and future employment options once they had earned their degree. The results of these questions can be found in Table 22-24, respectively. Question eight asked if the student was currently employed. Thirteen of the 16 or 81.25% of the students surveyed responded "Yes," while 3 or 18.75% were not currently employed.

Table 22: (Question 8)

Employed

Employed	Number of students	Percentage
Yes	13	81.25
No	3	18.75

The next question was designed to expand on the previous question asking, if the student was employed, to explain what he did. Of the 16 surveyed 12 answered this question. The most common response was professor/teach, which accounted for 6 of the 12 responses or 37.5%. Four of the 12 students or 25% currently work in a technology-

based field using computers. One student was self-employed and another conducted health policy research.

Table 23: (Question 9)

What it is you do

Type of job	Number of students	Percentage
College Professor	6	37.5
Self-Employed	1	6.25
Computer related	4	25
Policy Research	1	6.25
No Response	4	25

The tenth question of this section asked the students once they had completed their degree in which area did they plan to work in: public sector, private sector, teach, stay with current employment, or other. Ten of the 16 students surveyed or 62.5% expressed an interest in teaching once they completed their degree. Two students selected the public sector and another two students selected the private sector. There were two students who were undecided and were looking to explore their options once the finished.

Table 24: (Question 10)

Type of Employment once degree is completed

Type of employment	Number of students	Percentage
Public Sector	2	12.5
Private Sector	2	12.5
Teach	7	43.75
Stay with current employment	3	18.75
Other	2	12.5

Conclusions

This survey attempted to provide empirical data on the understanding of information privacy and the important issues involved from the viewpoint of students working toward a Ph.D. degree in Information Science at the University at Albany. The major findings from the study included:

- **87.5% of the respondents have purchased products on the Internet.**

This study co-insides with the general trend throughout the United States in that e-commerce accounts for a massive amount of revenue. An interesting finding from the question on the Internet and e-commerce is that even though browsers like Netscape and Internet Explorer feature encryption software 50% of the respondents had concerns about providing information such as credit card numbers over the Internet. Those that were not concerned, 37.5%, seemed to be aware of encryption technology as mention by their comments. Many of the respondents, 68.75%, also took precautions in purchasing online mentioning only using secure servers. One respondent went as far as to read the privacy statement on Web sites and look for the logos of TRUSTe and the Better Business Bureau to ensure her transactions were private.

- **When asked if the respondents had ever asked to be removed from a telephone solicitor's list 68.75% answered "Yes."**

Many of the respondents provided further comments to this question. A large number stated that such calls were annoying. Many solicitors target homes at night and many people do not want to be bothered with such telephone calls. One respondent stated that she uses a caller identification box to ensure she is not bothered with such telephone calls. Four out of five respondents commented on how easy it was to be removed from a

company's call list to ensure they would not be called again in the future. A simple statement to the telemarketing representative asking not to be called can save a person's time, limit abuse of personal information, and avoid further aggravation.

- **56.25% of the respondents have concerns about providing information to obtain a credit/debit card.**

The next major conclusion from this study focused on the respondents' concern about providing personal information to obtain credit/debit cards. 56.25% of the respondents had concerns about providing such information. Another conclusion that came about from the questions on credit/debit cards was that 50% of the respondents owned one additional card more than they used. The average respondent owned 3.75 cards and only used 2.3. The researcher believed people might keep additional cards in case of emergencies, whereby the card is seldom used.

- **100% of the respondents have requested that a company not share their personal information with other companies.**

The fourth major conclusion from this study centered on the respondents' request that companies not share personal information with other companies. Many companies now provide check boxes whereby a person may opt out from having their information shared with other companies. By taking part in this service an individual can eliminate his personal information from being rapidly spread about. In seeing a response rate this high, it shows that the respondents were taking steps to control where their personal information was going.

- **75% of the respondents had negative feelings about their personal information being bought and sold.**

The fifth conclusion was that 75% of the respondents had negative feelings about their personal information being bought and sold. In a society where the economy is constantly under scrutiny it is no wonder companies try to get an edge on their competition by purchasing and selling personal information on individuals. Many of the respondents wrote that they do not like this practice at all. One person wished he could control such situations better but as another respondent stated once she has given out the information it is no longer personal. With such a large percentage having negative views on this practice, many of the respondents exhibited an excellent knowledge and understanding of how information is used and practices needed to avoid having their personal information abused.

Future Research

This survey was limited to a very small population of Ph.D. students from the School of Information Science and Policy at the University at Albany. Though the population was small, the researcher if given the time, would have liked to administer the survey to all students within the School of Information Science and Policy as well as a sample of people from with in the community. In doing so the researcher would be able to examine those studying various aspects of information and those who are not. Such research would provide an interesting view on the level of privacy knowledge and understanding from both populations.

Notes

[1] H. Jeff Smith, *Managing Privacy*. (Chapel Hill: University of North Carolina, 1994) 7.
[2] Ellen Alderman & Caroline Kennedy, *The Right to Privacy*. (New York: Random House 1995, 1997) 323.
[3] Alderman & Kennedy 323
[4] State University of New York at Albany. *Information Science Doctoral Program*. (Princeton, NJ: Peterson's, 1999)
[5] State University of New York at Albany. *Information Science Doctoral Program*. (Princeton, NJ: Peterson's, 1999)
[6] Alderman & Kennedy 323-24.
[7] Ferdinand Schoeman, "Privacy Philosophical dimensions of literature" *Philosophical Dimensions of Privacy*. Ed. Ferdinand David Schoeman (Cambridge: Cambridge University Press, 1984) 2.
[8] Stefano Scoglio, *Transforming Privacy*. (Westport, Connecticut: Praeger, 1998) 2
[9] Scoglio 1-2.
[10] H. Jeff Smith 203.
[11] Amitai Etzioni, *The Limits of Privacy*. (New York:Basic Books, 1999) 118.
[12] H. Jeff Smith 203.
[13] Lisa Eckstein, *Privacy Journal*. "Zealous Fund Raising" (Providence, RI: Robert Ellis Smith) 21(5):3
[14] Eckstein, *Privacy Journal*. "Zealous Fund Raising" V. 21 N.5 p3.
[15] *Privacy Journal*. "Congress Out of Step on Social Security Numbers" (Providence, RI: Robert Ellis Smith) 22(12):1.
[16] Dianne Feinstein. "Personal Information Privacy Act, 105-1: S.600 (Washington: Government Printing Office, 1997)
[17] Feinstein. "Personal Information Privacy Act, 105-1: S.600
[18] Lawrence J. Goodrich, "Halting 'Identity Theft' in ERA of Internet Access" *Christian Science Monitor*. April 30, 1997. 89(108):3.
[19] THOMAS Legislative Information on the Internet. Washington D.C. 12 Nov. 1999 <http://thomas.loc.gov>
[20] H. Jeff Smith 43.
[21] H. Jeff Smith 43.
[22] Etzioni 128.
[23] David F. Linowes, *Privacy In America*. (Chicago: University of Chicago, 1989) 127.
[24] Scolglio 12.
[25] Jeffrey Rothfeder, *Privacy for Sale*. (New York: Simon & Schuster,1992) 97.
[26] Anne Wells Branscomb, *Who Owns Information?*. (New York: HarperCollins, 1994) 22.
[27] Scoglio 12.
[28] *Privacy Journal*, "Theft of Identity Rises to Thousands a Day" (Providence, RI: Robert Ellis Smith) 22(4):1.
[29] Rothfeder, *Privacy for Sale*. 79-80.
[30] Bronwyn Fryer, *Information Week*. 8/26/96 594:87.
[31] Fryer 87.

[32] Fryer 88.
[33] John Grossmann, *Sky* "Could John Grossmann have some privacy please?" (April 1998) 66.
[34] Grossmann 66.
[35] Carole A. Lane, *Naked in Cyberspace*. (Wilton, CT: Pemberton Press, 1997) 153.
[36] *Economist* "We Know You're Reading This". 1996. 338 (7952):27.
[37] *Economist* 27.
[38] Lane 155.
[39] Judith Wagner DeCew, *In Pursuit of Privacy*. (Ithaca: Cornell University Press, 1997) 146.
[40] DeCrew 148.
[41] Grossmann 66.
[42] Lisa Eckstein, *Privacy Journal*. "Mad About Telemarketing? Justice is on Your Side". (Providence, RI: Robert Ellis Smith) 21(3):1.
[43] Eckstein 1.
[44] Robert B. Gelman, *Protecting Yourself Online*. (New York: HarperCollins, Inc. 1998) 47-48.
[45] Etzioni 76.
[46] Etzioni 128.
[47] Jeffrey Rothfeder and Daniel Tynan, *PC World*. 1998. 16(9):96-105.
[48] Rothfeder and Tynan 96-105.
[49] Rothfeder and Tynan 96-105.
[50] Rothfeder and Tynan 96-105.
[51] Rothfeder and Tynan 96-105.
[52] Alderman & Kennedy 328.
[53] H. Jeff Smith 173.
[54] Etzioni 161.
[55] Etzioni 161 and 187.
[56] Rothfeder 89.

Bibliography

Alderman, Ellen and Caroline Kennedy. *Privacy and Information.* New York: Random House, 1995.

Bier, William C., ed. *Privacy: A Vanishing Value?* New York: Fordham University Press,1980.

Branscomb, Anne Wells. *Who Owns Information.* New York: Basic Books, 1994.

DeCew, Judith Wagner. *In Pursuit of Privacy.* Ithaca: Cornell University Press, 1997.

Dolan, Elizabeth M. and Irene E. Leech. "Privacy Issues on the World Wide Web." *Consumer Interests Annual.* 1997. 43: 200-203.

Carroll, John M. *Confidential Information Sources: Public and Private.* Boston: Butterwoth-Heinemann, 1991.

"Congress Out of Step on Social Security Numbers" *Privacy Journal.* Providence RI: Robert Ellis Smith, 1996: 22(4)

Eckstein, Lisa. *Privacy Journal.* "Zealous Fund Raising" Providence, RI: Robert Ellis Smith, 21(5):3.

Epstein, Richard A. "Privacy, Please: Thinking about a Troublesome Concept." *National Review.* 27 Sept. 1999 51(18):46-50.

Etzioni, Amitai. *The Limits of Privacy.* New York: Basic Books, 1999.

Feinstein, Dianne. "Personal Information Privacy Act, 105-1:S.600 Washington: Government Printing Office, 1997.

Fryer, Bronwyn. "Visa Crack Down on Fraud." *Information Week.* 26 Aug. 1996. 594: 87-89.

Gelman, Robert B. *Protecting Yourself Online.* New York: HarperCollins, Inc. 1998.

Goodrich, Lawrence J. "Halting 'Identity Theft' in Era of Internet Access." *Christian Science Monitor.* 30 Apr. 1997 89(108):3.

Grossman, John. "Could John Grossman have some privacy please? *Sky.* April 1998: 66-74.

Hannon. Neal J. *The Business of the Internet.* Cambridge, MA: Course Technology, 1998.

Appendices:

A: Survey
B: Institutional Review Board

I am Mark C. Scott, a Master's of Library Science student, completing my seminar paper requirement. The questions in this survey will comprise the data for my paper. These questions will measure some aspects of your control and use of your personal information. The survey should take no more than 15 minutes to complete. ***In no way will the information you provide be sold, distributed, or used in any way other than for the data analysis portion of the study. Your participation is voluntary. You do not have to answer any question you do not want. The information you provide will remain confidential and will only be reported in the aggregate.*** Discussion, explanation or elaboration of your answers in the blank spaces provided will be very helpful in my research. Thank you for taking the time to complete this survey.

Personal Information and the INF Ph.D. Student

Survey

Credit Cards and the Internet

1. How many credit cards/debit cards do you presently ***own***? _____

2. How many credit cards/debit cards do you presently ***use***? _____

3. If you own a credit card/debit card do you have any concerns about providing personal information to obtain these cards (e.g., mother's maiden name, social security number).

_____ Yes
_____ No

Comments:

4. The Internet is expected to account for more than $400 billion over the next three years. With the nature of our economy turning toward e-commerce, have you ever purchased a product on line?

_____Yes, please skip question 5 and answer questions 6, 7, and 8.
_____ No, please answer question 5 (and then skip to next section).

5. Is there a particular reason why you do not purchase products on line? (Please skip to the next section on Data Lists)

6. If yes, how many times have you made purchases over the Internet? _____

(Please continue on page 2)

7. Do you have any concerns about providing personal information (e.g., credit card number) over the World Wide Web? Please explain.

8. Do you take any precautions (accept or reject particular sites when purchasing over the Internet)? What precautions do you take? If you answered "no," why not?

Data Lists

1. In a given month how many magazines or journals does your household receive in the mail? _____

2. In a given month how many catalogs does your household receive in the mail? _____

3. On average how many telephone solicitations do you receive in a month? _____

4. Have you ever asked to be removed from a solicitor's phone list?

_____ Yes
_____ No

If you answered "yes," why did you want to be removed, and was it an easy process? Comments?

(Please continue to page 3)

5. Companies throughout the country are constantly purchasing and selling consumers' personal information. How do you feel about your personal information being bought and sold (i.e., address, interests)? Comments:

6. Have you ever requested that a company not share your personal information with other companies?

_____ Yes
_____ No

Comments:

7. In your experience have there been times in which you feel sharing your personal information has been helpful for you? Please list or describe these experiences.

8. Have there been conversations, experiences, or other outside forces throughout your life that have led you to deal differently with your personal information? (Or do you place your personal information into the world freely?)

9. The Social Security Number is used as an identifier for educational, financial, and other areas of life. What precautions, if any do you take in giving out this number? Have you ever experienced a situation where your number was abused? Please explain

(Please continue on page 4)

Questions about you

1. What age range best describes you?

_____ 20 – 29
_____ 30 – 39
_____ 40 – 49
_____ 50 – 59
_____ 60 or older

2. Are you:

_____ Female
_____ Male

3. Are you:

____ Single
____ Married
____ Divorced

4. Do you have any children living in your household?

____Yes
____No

5. If yes, place a number in each category next to the appropriate age group:

____ 0-8
____ 9-12
____ 13-19
____ 20-25

6. Please indicate your country of citizenship.

7. Please indicate the milestones you have completed in the Ph.D. program.

____ 701
____ 702
____ 703
____ 704
____ Comprehensive examinations
____ Major specialization qualifier
____ Minor specialization qualifier
____ Proposal defense
____ Dissertation defense (essentially done waiting to graduate)

(please continue to page 5)

8. Are you currently employed?

____Yes
____No

9. If yes, what is it that you do? Please explain.

10. Once you have successfully defended your thesis and earned your Ph.D., where do you plan to work?

____ Public Sector
____ Private Sector
____ Teach
____ Stay with current employment
____ Other, please describe _____

Thank you. Please staple this survey and return to Mark C. Scott.

If you have any questions or concerns please call
Professor Deborah Andersen at 442-5122 or by email at
dla@cnsvax.albany.edu
or
Mark Scott at ms3004@cnsvax.albany.edu

If you have any questions concerning your rights as a subject you can call 442-3510.

Office for Research

Appendix B inistration 216
Albany, NY 12222

518/442-3510
Fax: 442-3560

UNIVERSITY AT ALBANY
STATE UNIVERSITY OF NEW YORK

TO: Mark Scott

FROM: Institutional Review Board

DATE: November 3, 1999

SUBJECT: **REVIEW OF PROTOCOL #99-368**
ENTITLED: "Personal Information and the INF Ph.D. Student""

After the University at Albany Institutional Review Board (IRB) reviewed the above-referenced protocol under the expedited review process, it was determined that it involves human subjects who will not be at risk and has given final approval effective November 1, 1999.

This approval is valid for one year only. You must request a continuation of the approval if the activity lasts more than one year.

If you question any of these determinations, you have the option of requesting a full review by the IRB which will make the final determination. NOTE: The IRB may request a full review to reconsider any protocol approved under expedited review, You will be notified in advance of this review.

If you have any questions regarding the review of your protocol, please do not hesitate to contact me.

Cheryl Savini
Research Compliance Administrator
On behalf of the IRB

Att: 1
Cc: D. Anderson

INSTITUTIONAL REVIEW BOARD
APPROVAL CONDITIONS

- This approval applies **only** to the protocol referenced in the attached memo.
- It is incumbent on you to secure the prior approval of the Board for any changes in your proposed procedures that will affect your use of human subjects.
- You must report to the Board any problems that arise in connection with your use of human subjects in this activity.
- If you have any questions concerning the determinations, you have the option of requesting further review by the IRB which will make the final determination.
- The IRB may request a full review to reconsider any protocol approved under expedited review. You will be notified in advance of this review.

APPROVAL OF THIS PROTOCOL BY THE IRB ONLY SIGNIFIES THAT THE PROCEDURES ADEQUATELY PROTECT THE RIGHTS AND WELFARE OF THE SUBJECTS AND SHOULD NOT BE TAKEN TO INDICATE UNIVERSITY APPROVAL TO CONDUCT THE RESEARCH.