

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	1
Introduction	2
The School of Information Science and Policy	3
Purpose of the Study	4
Hypotheses	4
Limitations of the Study	5
What is privacy?	6
Social Security numbers	8
Abuses of the Social Security number	9
Credit Cards	11
Data Lists	14
Privacy and the Internet	17
The Public and Private Sectors	21
Research Methodology	23
Survey Results	25
Conclusions	41
Future Research	43
Bibliography	46
Appendices	49
A: Survey	
B: Institutional Review Board	

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 one's 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 people's 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 one's 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., Experian, 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