

PREFACE

Introduction

Much has been written about the disadvantages to student learning at large research universities (e.g., Pukkila 2004). This book was borne out of a belief that research universities can add unique elements to student education. By learning how to conduct research and carrying it out, students improve their general thinking skills and develop abilities that carry over to all other aspects of life.

Systems majors need – and are given – strong technology skills in their classes. However, with great knowledge come great responsibilities. In the privacy and technology class that brought this book into being, students focused on extending the depth of their technical knowledge while further developing their sense of ethics related to the technologies they will ultimately be charged with developing and managing.

One of the tools the students used to analyze technology related ethics is a categorical tool dubbed PAPA (Mason 1996). The four categories of PAPA are *privacy*, *accuracy*, *property*, and *accessibility*. The first category, *privacy*, was the main focus of the class, and one on which all papers in this volume focus. Privacy refers to the information about self an individual is willing or forced to give up, and the class agreed on the following definition for most of the chapters:

.a. The state or condition of being withdrawn from the society of others, or from public interest; seclusion. b. The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion. Also attrib., designating that which affords a privacy of this kind (OED 1993).

The second category of PAPA, *accuracy*, deals with data quality, which the class defined as intrinsic, contextual, and representational data quality (for details see Strong, Lee, and Wang 1997). Property examines ownership details, exchange fairness, and access characteristics, whereas accessibility addresses the digital divide of information between the haves and the have-nots. These four categories were used in many chapters to consider the implications of the different types of technologies analyzed.

Survey

To tie together the topics of the different groups, a class survey was designed. Each group contributed a set of 7-point Likert-type statements related to their topic, which were added to Smith et al.'s (1996) privacy items. The students collected a set of 517 valid surveys, which was then submitted to basic data analysis.

Demographics	Statistics
Age	Mean = 2.27 – 100 18-20yr, 273 21-30yr, 86 31-40yr, 31 41-50yr, 24 51-60yr, 6 61-70 yr.
Gender	Mean = 1.46 – 239 women and 278 men
Internet experience	Mean = 4.97 – 7 0-3yrs, 513 > 3yrs

Age. With advancing age, respondents were more willing to be under video and audio surveillance as long as it made them feel safer.

Somewhat surprisingly, there was a strong positive relationship between the age of the respondent and extent to which they did not worry about their privacy related to radio frequency ID (RFID) chips used in retail stores. These findings are especially interesting given the general tendency in the U.S. for erosion of privacy concerns among young people. Further disagreement between age groups is found in the question of whether DNA samples related to paternity tests should be shared with others. Young respondents tended to agree that such samples should never be used for other purposes. This may simply be a matter of stake as such problems are more likely to impact young people.

Gender. Women were less likely to accept being monitored through video and audio surveillance and felt that companies should go to greater lengths to ensure the data quality of their consumer information. In general, women were also more concerned about having to give up private information to companies than were men.

An interesting – and consistent – finding was that men were much more likely than women to trade away their privacy if given something in return. This finding may have great implications for marketing companies, suggesting that finding the right item to give away may be vital to getting men to give up their private information. On the other hand, social network approaches may work better in terms of enticing women (Monge and Contractor 2003).

Men were also more likely to feel comfortable in conducting financial business over the Internet. They were also stronger in their belief that companies should never use personal information for anything but the original purpose, i.e. for secondary uses. They were also more likely to accept the website tracking conducted by online companies, as well as less likely to regard their medical information as highly confidential.

Strong opinions. Some items in the survey turned out to be real button-pushers to respondents. Companies would do good to heed these before making privacy related decisions. The top five items are outlined here:

- 1) Companies should never sell personal information in their computer databases to other companies (6.35).
- 2) Companies should take more steps to make sure that unauthorized people cannot access personal information (6.26).
- 3) Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs (6.12).
- 4) Companies should take more steps to make sure that the personal information in their files is accurate (6.06).
- 5) Companies should not have the right to use video and audio bugs without employees knowing (5.94).

It seems clear that of all the statements the respondents could have strongly agreed with, these five all share something in common.

Statements (1) through (3) are about what companies should do with the consumer information they have already stored. Namely, companies should protect such information from outside entities, whether from sale by the company itself or from unauthorized access to the information. Similarly, statement (4) suggests that it is important to respondents that companies keep the information about them accurate. Finally, responses to statement five state that consumers should be aware of what information is collected and how it is collected, especially when it comes to such intrusive technologies as video and audio surveillance. In short, the five items provide good guidelines for companies in the process of developing privacy policies.

Factor analysis

Furthermore, the results were factor analyzed to get a sense of the respondents' view of the relationships between the different topics. A principal component analysis using a varimax rotation showed that out of 52 components, 40 percent of the variance could be explained by the first five factors (selection supported by a scree plot analysis).

Table 2: Factor Analysis

Factors:	Privacy? I want security!	My Infor- mation!	I'm safe!	I trust them!	Do it right!
Items	1	2	3	4	5
It's ok for stores to track my purchases without giving me a discount or some other kind of reward.	0.79				
The information that I provide to websites will not be monitored or modified by any unauthorized individuals.	0.77				
The information that I provide is stored in a secured place by websites.	0.77				
I would make transactions through websites even if they do not have a privacy/security seal (such as being "Hacker-Free").	0.66				
My bank account information is very safe and secure from theft, when I type it into my computer.	0.64				
National ID cards improve national security.	0.63				
I would use my company email account to plan or discuss subversive activity against my company.	0.56				
Putting the public under video/audio surveillance makes me feel safer.	0.56				
I am concerned that there is currently no legislation governing the use of radio frequency identifiers by manufacturers.	-0.51				

Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.	-0.46				
I do not believe there is any way to change ballots cast into a computerized electronic voting machine.	0.44				
A national ID card would not affect my daily life.	0.43				
Companies should devote more time and effort to preventing unauthorized access to personal information.		0.65			
Companies should never sell the personal information in their computer databases to other companies.		0.63			
Companies should take more steps to make sure that unauthorized people cannot access personal.		0.62			
It bothers me to give personal information to so many companies.		0.61			
When companies ask me for personal information, I sometimes think twice before providing it.		0.61			
Companies should take more steps to make sure that the personal information in their files is accurate.		0.61			
Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs.		0.58			
Companies should have better procedures to correct errors in personal information.		0.56			
It usually bothers me when companies ask me for personal information.		0.42			
I feel safe giving out my personal and financial information through websites.			0.75		
I feel comfortable conducting financial business, such as banking, over the Internet.			0.74		
The DNA samples I give to a company to perform a paternity test would not be shared with others upon request.			0.58		
Spyware removal software will protect me from identity theft.			0.51		
I would feel comfortable disclosing personal information via my corporate email account.			0.43		
My doctors are the only people with access to my medical records.				0.67	

If radio frequency identifiers are used in retail products, I am worried about the security of my personal information.					-0.63
It's ok for business to record and analyze my activities if it means they can offer lower prices.					0.41
When people give personal information to a company for a specific reason, the company should never use the information for any other reason.					0.64
Public areas and venues should be monitored with video surveillance in the interest of security.					0.60
Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.					0.46

Table 2 displays the results of an exploratory factor analysis of the class-facilitated survey (factor loadings below .4 suppressed). The analysis unearthed five factors. The first factor, named 'Privacy? I want security!', measures the belief that privacy is not very important for an individual, and all that matters is his or her belief in the security of the systems they use.

The 'My information!' factor depicts a desire to carefully protect own privacy, primarily by not sharing information with companies. In cases where the individuals do share their information with companies, they want companies to treat that information with respect, and not to share it with other entities.

The third factor, 'I'm safe!', speaks to the individuals' belief that their information is carefully protected in the society, be that by corporations or governments. It is unknown whether this belief is based on a conviction that authorities are responsible and trustworthy or a low valuation of personal information.

The fourth factor, 'I trust them', makes it very clear where the respondent stands. These respondents will give up their personal information without hesitation because they trust corporations and individuals to take care of their information in a responsible manner.

The fifth factor, 'do it right!', reflects a belief that, if companies or governments are taking away the individuals' privacy, they should be doing so correctly, with resulting good quality data. When making decisions, companies should take note of these different categories of attitudes towards privacy.

Conclusions

Overall, this book represents a great deal of hard work by many bright and talented individuals. By taking responsibility for individual topics and by becoming experts on the privacy related technologies of their choice, students have compiled an impressive set of papers. While not all of the papers are based on original research, even the descriptive ones provide valuable ideas and guidance.

Clearly, not all the contributions can be tallied here, but some interesting examples of excellent work includes Lassow and Ourada's chapter on the deception of grocery chains' customers by the stores creating a perception of savings related to grocery cards. In fact, consumers are roped into financing millions of dollars of operational costs for the systems while giving away their privacy at the same time. Interesting and potentially very useful to our government, Pham and Cuong's chapter develops an electronic bill of rights related to cookie use, whereas Dickey and Al-Hinai develop a case study of the consequences of implementing a national ID card system in Oman. Perhaps the most frightening scenario in the book is developed by MacGregor and Wagner, who point out that most email sent and received by consumers is actually owned by corporations and organizations. This fact, combined with new developments in automatic analysis of text allows profiling of consumers at a never before seen wholesale level, especially in terms of the quality of profiles that will be available.

All the papers in this volume impart useful knowledge, and only a thorough reading will provide access to the rich wealth of thinking. Perhaps, more important than what is contained in this volume, are the skills gained by the students themselves. As these students go into industry, their skills and knowledge will undoubtedly greatly benefit their companies.

Kai R. Larsen
Leeds School of Business
University of Colorado, Boulder
December, 2004

Works Cited

- OED (1993), *The Compact Oxford English Dictionary*, Oxford: Clarendon Press.
- Mason, Richard O. (1986), "Four Ethical Issues of the Information Age," *MIS Quarterly*, v. 10, n. 1, pp. 5-12.
- Monge, Peter R. and Noshir S. (2003), *Theories of Communication Networks*, New York: Oxford University Press.
- Pukkila, Patricia J. (2004), "Introducing Students Inquiry in Large Introductory Genetics Classes," *Genetics*, v.166, pp. 11-18.
- Smith, H. Jeff, Sandra J. Milberg, Sandra J. Burke (1996), "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, v. 20, n. 2, pp. 167-196.
- Strong, Diane M., Yang W. Lee, and Richard Y. Wang (1997), "Data Quality in Context," *Communications of the ACM*, v. 40, n. 5, pp. 103-110.