2006

Consumer concerns towards privacy: An empirical study

Maria Nicolaou

CONSUMER CONCERNS TOWARDS PRIVACY: AN EMPIRICAL STUDY

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Interdisciplinary Studies

---

by

Maria Nicolaou

December 2006

CONSUMER CONCERNS TOWARDS PRIVACY:

AN EMPIRICAL STUDY

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Maria Nicolaou

December 2006

Approved by:

[redacted]

Dr. Nabil Razzouk, Chair, Marketing

11-27-06

Date

[redacted]

Dr. Victoria Seitz

ABSTRACT

Informational privacy invasion issues have recently gained significant attention from businesses, lawmakers, governments, activists, and most importantly consumers. Innovations such as Customer Relationship Management and Radio Frequency Identifiers have been key technologies associated with this loss of privacy. Hence, the purpose of this study was to determine the influence of demographics on attitudes towards privacy. An instrument was developed and a convenience sample of university students was tested. Results showed that educational background played a role in the way that participants perceived the applications of RFID.

ACKNOWLEDGMENTS

I would like to express my appreciation to the people who supported me throughout this long-term process. My special thanks go to Dr. Razzouk and Dr. Seitz who encouraged me and guided me towards the successful completion of this thesis.

I would also like to thank my family, who even though they were miles away from here, they were next to me in every step of this process.

I am also very thankful of all the wonderful friends I am blessed in having in my life. Thank you for your continuous support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

Background

In 1949, George Orwell delved into a contemporary and contentious issue, the issue of privacy, when he published his visionary and farsighted book "1984". "BIG BROTHER IS WATCHING YOU" (Orwell, 1949, p. 3) is a memorable phrase from the book, the meaning of which goes beyond its seeming. The novel may be described as a prophecy for the present times. In fact, Rehnquist (2004) quotes Orwell who said that "I do not believe that the kind of society I describe necessarily will arrive, but I believe (allowing of course for the fact that the book is a satire) that something resembling it could arrive" (p. 985). Moreover, Rehnquist (2004) concludes by saying that "the book stands as a warning against letting liberal democracy slip away or be extinguished" (p. 987).

"1984" revolves around a society where the free act of the human body and mind is proscribed by the governmental hegemony. Every act and every thought is monitored and scrutinized by the Thought Police, and even news is filtered by the Ministry of Truth. The structure of the "1984" society is ordained to create an austere and

constrained culture for Big Brother to dictate the country. Big Brother seeks to vanish any privacy that the people may have to create homogeny and control.

In the present times, privacy is not only a privilege of every citizen, but it is a fundamental civil right. For this reason in many countries, privacy is protected by laws and regulations.

Privacy in the United States

In the United States, the concept of privacy dates back to the founding of the Constitution. Even though the notion of privacy is not explicitly protected by the Constitution, the First, Third, Fourth, Fifth and Ninth Amendments infer to the right to privacy (Clarkson et al., 2001, p. 83)

However, the issue of privacy was directly addressed for the first time in American society in 1890, when Samuel Warren and Louis Brandeis published their article "The Right to Privacy", in the Harvard Law Review. The two authors agreed that "the individual shall have full protection in person and in property is a principle as old as the common law" (p. 1). However, they argued that it was necessary to modify the common law according to the transformations that took place in society regarding

"political, social, and economic" issues (Warren & Brandeis, 1890, p. 1). Moreover, the authors provided a summary of all the adjustments that had been made in the law system regarding the right to privacy to abide by societal changes. For example, in the beginning the right to life and property was sufficient to protect individuals' freedom and land (Warren & Brandeis, 1890, p. 1). In later years, the need for "recognition of man's spiritual nature, of his feelings and his intellect" became essential (Warren & Brandeis, 1890, p. 1).

Nowadays, as Tavani (1999) mentions there is a new kind of privacy: "informational privacy" (p. 138). He argues that technologies such as Data Mining are linked with this specific kind of privacy.

The years following the article by Warren and Brandeis were constructive regarding passing new laws. California, New York, Pennsylvania and Utah adopted new statutes that adhered to the understanding of privacy as Warren and Brandeis explained (Gormley, 1992, p. 11).

Further in 1974, the United States adopted the Privacy Act to regulate the circulation of personal information. The Act covers among other issues, the subject of conditions of disclosure, access to records,

mailing lists, civil remedies and criminal penalties. As specified in the Act:

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. (United States Department of Justice [USDOJ]).

The Act protects individual information from spreading to the public or from dispersing from business to business. As a result, many other laws have been adopted in the past two decades, such as: the Gramm-Leach Bliley Act, the Fair Credit Reporting Act, the Computer Matching and Privacy Protection Act, and the Privacy Principles (Federal Trade Commission [FTC]).

Privacy, Security and Technological Innovations

Although the protection of privacy has gained significant attention at both the national and international levels, the phobia regarding terrorism and crime in many countries has altered the manner in whereby a country defends this constitutional right. Gates (1996) justifies that "the prospect of so many cameras, always

watching, might have distressed us fifty years ago, as it did George Orwell" (p. 306). But nowadays, "almost everyone is willing to accept some restrictions in exchange for a sense of security" (Gates, 1996, p. 306). He exclaims, "it is a question of balance" (Gates, 1996, p. 307).

Even though, the year of 1984 did not corroborate Orwell's foretelling for a society like the one of Big Brother, the emergence of technological innovations in 1980s increased concerns about privacy. While in "1984" people did not have the freedom of mind to be concerned about their future, nowadays "people want to understand how [information technology] will make the future different, whether it will make our lives better or worse" (Gates, 1996, p. 284). To the same degree that Gates states his optimism about the impact that information technology has on the human culture, he also articulates a realistic point of view. Specifically, he explains that

> societies are going to be asked to make hard choices about the universal availability of technology, investment in education, regulation and the balance between individual privacy and community security...The power and versatility of digital technology will raise new concerns about individual

privacy, commercial confidentiality, and national security (Gates, 1996, p. 285).

In spite of the fact that a society like the one in "1984" can be criticized and condemned by any individual today, the concept of sacrificing privacy for other benefits is already instituted in the public and private sector.

Both the government and the private sector are in desperate need (for different reasons) to unveil individuals' actions by monitoring and examining different aspects of their lives. Some of these aspects include the passports, driver's licenses, credit cards, airline tickets, and rental cars.

Privacy in the Altar of Terrorism

For government purposes, when homeland security becomes an issue, privacy becomes a secondary matter. For instance, the United States government, due to recent terrorist threats, deliberated on the need to create a plan called Total Information Awareness program. The plan was to foresee terrorist attacks by using Information Technology to conduct human analysis and pattern recognition from data obtained through commercial transactions such as credit card purchases and telephone

calls. This new program triggered controversy between the government and activist groups.

Cain (2002) acknowledges that since the terrorists' attacks in the United States, privacy issues have become not only a consumer concern, but also a matter of national security (p. 23). Cain (2002) explains that the Federal Aviation Administration (FAA) will "employ racial profiling to distinguish the level of security checks imposed on individuals" (p. 25). Further, racial classifications are considered legal only if they serve governmental interest (Cain, 2002, p. 25). Even though, "no level of security risk would justify heightened security measures based exclusively on race under the US 14th Amendment Equal Protection concept", it is very likely that race could be a major issue during a government investigation (Cain, 2002, p. 25).

Another concern that Cain (2002) identifies is the usage of technological instruments for facial scanning and recognition (p. 25). Such technology may instigate "racial profiling rather than exercising legitimate law enforcement discretion" (p. 25). This may lead individuals of a specific ethnic background to the conclusion that they are being discriminated against and monitored.

Privacy and Consumer Confidentiality

Despite racial classifications in national security applications, another aspect of privacy that Big Brother did not infringe, but Gates brought attention to in 1996, is consumer confidentiality (p. 285). Confidentiality of customers' personal information is a major concern for customers as well as businesses that are threatened by various national and international privacy protection laws. In some parts of the world like Europe, the free and exposed use of consumers' data is strictly admonished (Whitman, 2004, p. 26). More precisely, as Whitman (2004) elucidates, "Europeans have aggressively condemned traffic in consumer data: It is, European lawyers believe, a serious potential violation of the privacy rights of the consumer if marketers can purchase data about his or her preferences, and regulation is thus imperative" (p. 26).

According to Whitman (2004), Europeans are more concerned about releasing personal information, especially credit reports, to businesses because privacy is an issue of dignity (p. 26). On the contrary, in the United States, people are more acceptant of the benefits that free trafficking of consumers' data may dispense (Whitman (2004, p. 26). For Americans, as Whitman (2004) distinguishes, privacy is an issue of liberty (p. 40).

Currently, these differences in laws and values may not create any concerns. However, it is safe to assume that the globalization era that the business world is experiencing will lead to clashes between privacy laws in different continents and countries (i.e. European Privacy Directive Vs USA privacy laws).

The sudden need to retrieve customers' personal information derives from the latest shifts in management. Major corporations recently introduced Customer Relationship Management (CRM), is being discussed, implemented and evaluated daily (Berry & Linoff, 2000). As an opportunity to increase profits companies need to emphasize customer service with customer loyalty. The ultimate goal is only achievable through personalization and a one-on-one relationship between the company and the customer. "Good customer relationship management requires understanding who your customers are and what they like and don't like" (Berry & Linoff, 2000, p. 14).

As opposed to mass marketing, companies target their customers individually based on their profile. This means that acquisition for customers' information is needed to create a customer's profile. Customers provide companies with their demographic and personal information and in return they receive personalized service that relates

directly to their needs and demands. In other words, CRM is beneficial for both the company and the customer. "Instead of having to buy every household in the United States with mass media to advertise a car or other item, companies will be able to buy the demographic that's most efficient to reach their potential customers" (Gates, 1999, p. 230). In the same respect for customers, "targeted ads should make consumers happy" (Gates, 1999, p. 231).

Data Mining

The breakthroughs in recent technology have generated an innovative way for interested parties to obtain useful and accurate information. Data mining strategies are designed to assist in the process of data acquisition, with the help of different techniques and algorithms. More specifically, data mining is able to extract "meaningful patterns and rules from large quantities of information" by classifying, estimating, and predicting (Berry & Linoff, 2000, p. 10). The reasons for using data mining may be constructive, but like any other breakthrough it can also initiate concerns. In this case, data mining relates back to the concerns of privacy. Since data mining is the means for more effective Customer Relations

Management, as well as management of large quantities of data, directly affects the issue of privacy. Tavani (1999) concludes that

> one reason why such techniques cause privacy concerns is because individuals are often not aware that data about them which they may have authorized for collection and use in one context is being mined, in ways they had not explicitly authorized, into information that is useful to certain businesses and organizations. (p. 144)

In recent years businesses have come to realize that keeping a customer actually costs less than trying to recruit new customers. With this in mind and with the help of data mining, organizations are able to forecast which of their clients are more likely to transfer to a rival company. With this kind of knowledge, companies can tailor their services to fit customers' needs and demands. As a result, the cycle of Customer Relationship Management begets benefits for the company and the customer.

However, the dilemma ascends when customers realize that they have to give up their private information to companies to enjoy the benefits of CRM.

Purpose of Study and Research Questions

Given the above, the purpose of the study was to determine consumers attitudes toward privacy and the influence of demographic factor on these attitudes. Previous research on privacy suggests a great difference on privacy ideologies between cultures (Whitman, 2004), income (Graeff & Harmon, 2002) and gender (Graeff & Harmon, 2002). As Monshi and Zieglmayer (2004) conclude, "different cultures and epochs understand privacy in radically different ways" (p. 312).

Specifically, the objectives of the study were to: 1) determine consumers' attitudes, knowledge and awareness regarding privacy issues, 2) determine the willingness to disclose selected individual information items, 3) determine the willingness to disclose selected individual information in specific situations, 4) determine the awareness and acceptance level of RFID technological innovation that relate to privacy, 5) determine demographic characteristics of respondents, 6) determine the influence of demographic characteristics on attitudes towards privacy.

The following research questions were addressed in the study:

R1: How do demographic variables play a role in the way an individual perceives informational privacy? For example, are perspectives on privacy ingrained on individuals based on their demographics?

R2: What is the relationship between the demographic variables and the awareness/knowledge of privacy issues?

R3: What is the relationship between demographic variables and individuals' willingness to disclose personal information in specific scenarios?

Limitations of the Study

The study was limited to a population of students from a southwestern university. Further, the study was limited to selected scenarios regarding privacy and awareness of Radio Frequency Identifiers.

CHAPTER TWO

LITERATURE REVIEW

Introduction

As a wave of new technology comes ashore, a new concept in business emerges with information technology as a means to create innovative strategies in customer acquisition and service. Customer Relationship Management (CRM) has come along to bridge the relationship gap between customers and businesses (Berson, Smith, & Thearling, 1999, p. 44). The bridge is aimed to draw both consumers and businesses into one meeting position where demands can be satisfied and profits can be reached.

However, along with every innovation there is a dilemma. In this case, CRM faces the issue of customer privacy - a concern, galvanized by almost every technological breakthrough. Businesses must realize that the cost of obtaining and networking consumer information could ultimately dissipate the privacy of consumers, which will lead to distrust (Hubbell & Redding, 2003, p. 49). Yet, the benefit of passing consumer information by businesses could generate a sustainable competitive advantage and more market share.

CRM operates in accordance with data mining strategies by obtaining private information from consumers and then using it in a way that "can yield important insights including prediction models and associations that can help companies understand their customers better" (Chye & Gerry, 2002, p. 5). "As businesses expand, however, that degree of intimacy is no longer available", so many companies count on the employment of CRM to bring them a step closer to their customers (Chye & Gerry, 2002, p. 4). On the other hand, customers get to enjoy the convenience that is designed for them.

Conversely, in spite of the customers' convenience there is a "fear that there is an inequity in the exchange equation leading to companies collecting and using personal information in unacceptable ways" (Fletcher, 2003, p. 251). Fletcher (2003) implies that even though customers release their information with the promise that they will receive higher quality service and their demands will be met, companies are the ones that actually benefit the most out of this equation (p. 13). This inequality may generate negative results due to the release of customers' information and lead to concerns about privacy that will consequently interfere with the success of CRM (Fletcher, 2003, p. 259). Specifically, Fletcher (2003) lists the

following outcomes: "loss of trust, irreparable damage to reputation and user retention, loss of revenue and new business, interruption of cross-border data flows, government/EU enforcement actions, litigation from consumers, privacy advocates and so on, civil and criminal penalties for wrongful disclosure, high cost of data protection software to ensure transparency and so on" (p. 260).

Defining Customer Relationship Management

Customer Relationship Management has been defined by many scholars in similar ways. Berson et al. (1999) define CRM as the "process that manages the interactions between a company and its customers" (p. 10). Among the same lines, Berry and Linoff (2000) described CRM as "the term that has come to embody much of what used to be called one-to-one marketing, along with ideas about sales force automation and customization" (p. 14). Chye and Gerry (2002) define CRM "as the process of predicting customer behaviour and selecting actions to influence that behaviour to benefit the company, usually leveraging on information technology and database-related tools" (p. 3). The authors state, among others, the following objectives of CRM as to a) to create a closer relationship with the

customers by analyzing data, and b) to "transform the company into customer-centric organizations with a greater focus on customer profitability as compared to line profitability" (Chye & Gerry, 2004, p. 4).

By the same token, Kavali, Tzokas, and Saren (1999) define relationship marketing as

> the process of planning, developing and nurturing a relationship climate that will promote a dialogue between a firm and its customers which aims to imbue an understanding, confidence and respect of each others' capabilities and concerns when enacting their role in the market place and the society. (p. 583)

Based on their definition the authors promote trust between customers and organizations, setting it as the foundation of their relationship.

Customer acquisition versus customer retention is an issue that marketers struggled with from traditional marketing to contemporary marketing. When CRM was introduced to the business world, ideas were shifted and the prevailing notion was that profits were expanded through customer retention. Winer (2001) concurs with the new perspective on customer retention and proposes a model that offers seven factors that help form a complete CRM that include: a database of customer activity, analyses of

the database, decisions about customers to target, tools for targeting the customers, building relationships with the targeted customers, privacy issues, and metrics for measuring the success of the CRM program (p. 4).

The first step suggests the creation of a database that will form a customer profile. In the profile such information should be included: transactions, customer contacts, descriptive information, and response to marketing stimuli (Winer, 2001, p. 4). With the use of planned model, Winer (2001) explains that companies with more interactions with their clients (i.e. banks and retail) are more likely to have better databases and, thus profiles on their customers (p. 24). The idea behind this model is that the more interaction there is between the organization and the clients the more information can be collected in order to form a more precise profile (Winer, 2001, p. 4).

Analyzing the data is the second component. In the past, marketers had the tendency to create groups of customers and then target them as a whole, whereas now each customer is viewed and targeted separately (Winer, 2001, p. 7). "Life Customer Value" (LCV) is used to identify the profitability of each customer by predicting "future purchasing, product and marketing costs, as well

as how long the customer can be expected to remain with the firm" (Winer, 2001, p. 8).

Customer selection is another important factor that helps target only those clients that appeal to the company's programs. "The goal is to use customer profitability analysis to separate customers that will provide the most long-term profits from those that are currently hurting profits" (Winer, 2001, p. 9). Ultimately, the company's goal is to spend time, effort and money into customers that are profitable to the organization.

The next step is targeting customers through the use of the right tools. Winer (2001) points out that there are a lot of new ways to target customers. Television, radio and print advertising are traditional ways of targeting, yet do not reflect personalization encouraged by CRM (Winer, 2001, p. 9). Instead, other ways like telemarketing, direct mail and the Internet are better methods for achieving the one-to-one relationship desired (Winer, 2001, p. 10).

In addition, relationship programs are another method of approaching customers and creating databases. This stage is very competitive since customers decide to maintain a relationship with a company based on the

loyalty programs and rewards offered to them (Winer, 2001, p. 12). "The overall goal of relationship programs is to deliver a higher level of customer satisfaction than competing firms deliver" (Winer, 2001, p. 12). Customer satisfaction is often related with positive outcomes, so marketers need to "develop programs that help to deliver performance beyond targeted customer expectations" (Winer, 2001, p. 12).

Customer service is essential in the formation of CRM. Every time a customer comes in touch with the organization, it could mean additional information for the database and repeat purchases (Winer, 2001, p. 13). Customization of products (Winer, 2001, p. 14) and the formation of a sense of community (Winer, 2001, p. 15) are additional ways that companies can use to attract their customers (Winer, 2001, p. 13).

The last component in creating a database is the metrics of an organization. "In a CRM world, increased emphasis is being placed on developing measures that are customer-centric and give managers a better idea of how their CRM policies and programs are working" (Winer, 2001, p. 17).

Winer (2001) concludes by saying that the "CRM practice is still far short of ideal" (p. 18). If

companies keep paying attention to those components that will lead to a more successful implementation of CRM, then the results will be positive and productive. Each organization may develop different approaches to improve their practices of CRM. These approaches may be the creation of new lead positions and better customer service (Winer, 2001, p. 18).

Privacy, Trust, and Loyalty

Gormley (1992) explains that throughout the years many scholars attempted to define privacy, without reaching a common ground (p. 3). However, even though the definitions of privacy vary, there is not one-way to define it. As Warren and Brandeis (1890) stated, the law (in this case the legal definition of privacy) will keep developing and changing according to the needs and changes of society (p. 1). Likewise, Standler (1997) agrees that privacy is indeed "an evolving area of law" (p. 2). He plainly defines privacy as "the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities" (Standler, 1997, p. 1).

Kavali et al. (1999) consider the ethical dilemmas that marketers deal with, especially since the introduction of Relationship Marketing. Their objective was to emphasize the difference between rhetoric and reality in Relationship Marketing and to point out ethical problems that relationship marketing may induce in decision-making.

What they found was effective Relationship Marketing (RM) could lead to a competitive advantage, but that trust, equity, responsibility and commitment were also an important part of it (Kavali et al., 1999, p. 577). The authors praise such characteristics because they can be used to prevent ethical dilemmas in business (Kavali et al., 1999, p. 577). Based on these characteristics they reasoned that "RM theory has the potential to contribute significantly to an improved ethical behaviour by affecting categories of ethical problems and preventing a number of them from arising in the first place" (Kavali et al., 1999, p. 577). They justified this argument by explaining that now, with the emergence of Relationship Marketing, customer satisfaction becomes the priority of good business that encourages ethical behavior (Kavali et al., 1999, p. 578). Further, they continue to explain that Relationship Marketing also promotes ethical behavior

within a company's management system due to the fact that "the market inside the firm becomes equally important to the outside market" (Kavali et al., 1999, p. 585). The image that represents a company in the outside world is a reflection of the inside world of the company (Kavali et al., 1999, p. 585).

Besides the ethical behavior that Relationship Marketing may endorse, privacy issues remain a crucial concern triggered by Relationship Marketing (Kavali et al., 1999, p. 578). The extensive database warehouse with detailed customer profiles insinuate apprehension about invasion of privacy. However, this concern is difficult to smother due to the nature of Relationship Marketing and that there are still a lot of issues that need to be addressed.

Likewise, Evans (2003) pinpoints to the invasion of privacy along with other several social concerns instilled by the collection and use of personal information (p. 665). Evans (2003) characterizes databases as a promising opportunity for organizations to "capture information on customers in a useful and accessible fashion, enabling companies to identify individual customers, monitor their buying behaviour and to communicate with them on an individual basis, often with

personalised offers" (p. 669). He also describes database to be a "sort of surrogate for the type of tacit knowledge of customers that the corner shop of old would possess" (Evans, 2003, p. 669).

Due to the ability of marketers and technology to collect personal data, Evans (2003) associates Customer Relationship Management with the invasion of privacy (p. 666), and he explains that "customers are increasingly cynical about companies in general, in terms of an incremental decline in trust" (Evans, 2003, p. 669). According to the researcher, some of the privacy concerns include: information privacy, right to access consumer information, physical/interaction privacy, control and accuracy (Evans, 2003, p. 668). Further, he defines information privacy as "the extend to which individuals can control who holds their data, and what is done with it" (Evans, 2003, p. 671).

Grossman (1998) delved into a perspective that viewed relationships between customers and businesses as an interpersonal relationship and found that customer-business relationships have similar characteristics with interpersonal relationships (Dwyer et al., 1987; Levitt, 1983, as cited in Grossman, 1998, p. 29). Such characteristics are: exchange process, cost,

expectations, satisfaction and rewards (Grossman, 1998, p. 31). Through these relationships, firms have the opportunity to create a competitive advantage over other companies (Grossman, 1998, p. 32). Grossman (1998) suggests that loyalty and long-term commitment are essential traits in a customer-firm relationship (p. 42).

Further, Grossman (1998) and analyzes four phases of consumer-business relationship that need to be taken into consideration by marketers to have successful outcomes. The first phase is courtship (Grossman, 1998, p. 33) whereby company and customer exchange information with each other. During this phase both parties seek to find benefits from the relationship.

The second phase is called maintenance and it is considered to be a very crucial point in a relationship (Grossman, 1998, p. 36). Scholars often support that "it is far more expensive to win back a customer after they have left than it is to keep them satisfied in the first place" (Berson et al., 1999, p. 42). Grossman (1998) suggests that a company should focus on maintaining relationships with existing customers, because in the long run it is more profitable and guarantees long-term relationships (p. 37).

The next two phases are trust and commitment. Customers will commit themselves to companies they trust. Grossman (1998) specifies that "commitment is more likely to result from a feeling of having made an investment" (p. 42).

However, Cannon (2002) contends that while technology advances in favor of businesses, it also gives customers more reasons to be apprehensive about their privacy and to require more protection (p. 42). Customer Relationship Management gives the opportunity to businesses to create rich databases with customers' information. Moreover, Cannon (2002) notes that this advancement makes trust an essential value in the relationships between businesses and customers (p. 43). Businesses view Customer Relationship Management as technology, software, and hardware, but they put aside the fact that it creates relationships (Cannon, 2002, p. 43). Specifically, Cannon (2002) explains that "the role of database management as the vehicle for customer interaction has become a central strategic issue that reaches far beyond technology" (p. 43). The relationship and privacy factors attach a challenge for organizations in the execution of CRM. Companies should have the responsibility to "become the custodian of customer trust and protect the privacy of

their customer" (Cannon, 2002, p. 44). If trust is implemented by both sides, then the complexity of CRM in organizations will be less severe.

Privacy and Demographic Variables

Graeff and Harmon (2002) pinpoint that there has been limited research on consumer privacy regarding demographics (p. 304). Their study focused on consumers' familiarity with grocery store discount cards and on consumers' knowledge about how their personal data is collected. In a telephone survey among 480 consumers results showed that consumers are familiar with supermarket discount cards, but there were a difference in opinions about stores' intentions to offer discount cards (Graeff & Harmon, 2002, p. 307). Specifically, "younger consumers were less likely to mention loyalty and competitiveness...and more likely to mention data collection, and promotions" (Graeff & Harmon, 2002, p. 309). Lower income consumers indicated opposite results. In addition, male consumers showed more willingness to share personal information and displayed less privacy concerns than female consumers (Graeff & Harmon, 2002, p. 310). The researchers found that income was more related to consumers' privacy concerns than any

other (Graeff & Harmon, 2002, p. 310). Higher income consumers had greater concerns about how their information was being used, but also were more likely to make purchases using credit cards (Graeff & Harmon, 2002, p. 311). Conversely, the study showed that despite privacy concerns that consumers revealed, purchase behaviors did not seem to be affected by their attitude towards it (Graeff & Harmon, 2002, p. 314).

Regarding psychographic characteristics, Fletcher (2003) emphasizes trust and attitude issues, and points out the importance of them in the development of CRM. In an era where privacy concerns are rising, trust between companies and customers may be the key solution to any fears. Fletcher (2003) introduces a grid that explains how privacy concerns can interfere with the development of CRM (see Figure 1) (p. 255). The grid categorizes customers in four areas: activists, partners, sleepers, and silent majority. The four dimensions used in the model are knowledge, privacy awareness, trust, and attitude. The first two dimensions (knowledge and awareness) are based on the cognitive perspective of consumers, which measures their response in regards to "transparency (who is collecting what on whom), security of information collected, and liability (what happens if privacy is

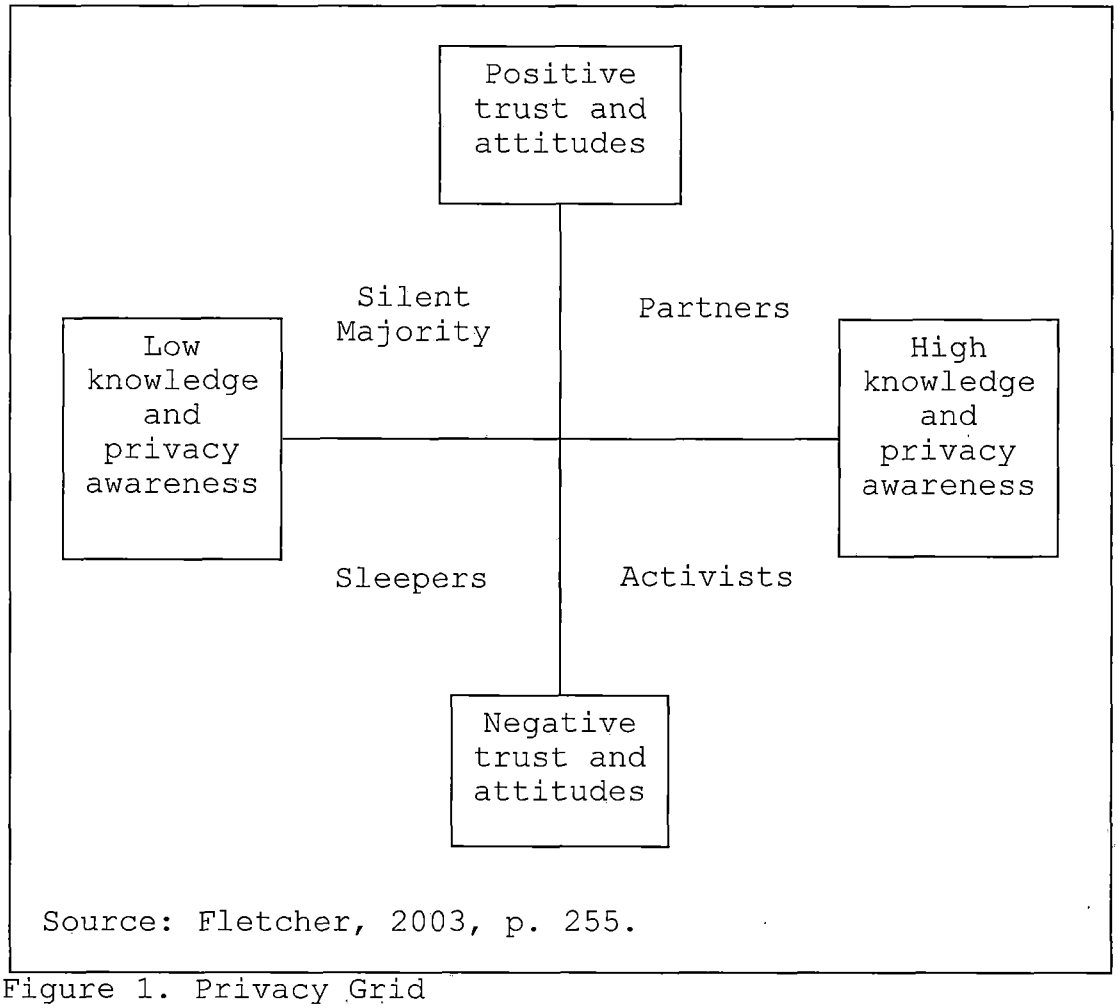

Figure 1. Privacy Grid

abused)" (Fletcher, 2003, p. 253). The last two dimensions (trust and attitude) are based on customers' past experiences with different companies (Fletcher, 2003, p. 254). Through this grid, Fletcher supports that CRM's success depends a lot on trust, loyalty and knowledge. This grid implies that customers have the power to control their relationships with different companies; therefore they influence the success of CRM. If companies fail to

create the feeling of trust between them and their customers, and to provide their customer with CRM knowledge then several consequences will follow. Such consequences are: "irreparable damage to reputation and user retention, loss of revenue and new business, litigation from consumers, civil and criminal penalties" etc (Fletcher, 2003, p. 259). Such consequences may deter the growth of CRM, confirm that customers have power over businesses and that they can use it for their benefit (Fletcher, 2003, p. 261). When customers fear that there is an inequality in the exchange of information between them and the company, they have the power and control of the situation. According to Fletcher (2003), marketers face a dilemma in their efforts to create relationships with customers (p. 261).

A second model by Fletcher (2003) analyzes how attitudes and trust affect business-customer relationships (see Figure 2) (p. 263). The model offers four situations

Table 1. The Different Market Situations Faced by Managers

	Positive seller	Negative seller
Positive buyer	Relationship ++	Exploitation +-
Negative buyer	Worm turns -+	Transaction --

Source: Fletcher (2003)

where companies and customers meet with either the same or different behaviors towards each other. These situations are: Relationship segment (where business and customer wish to create a relationship with mutual efforts and rewards), worm turns segment (where the business wants to create a relationship, but the customer wants only a transactional relationship), exploitation segment (where business wants a short-term transaction, but the customer hopes for a relationship), and transaction segment (where both parties enter for a short-term transaction)(Fletcher, 2003, p. 263). This model recapitulates the dilemma of marketers in their efforts to understand their market and target it in the most appropriate ways that lead to successful CRM.

Singh and Hill (2003) studied the privacy concerns, and in particular Internet privacy, of German consumers across demographic variables. The population was 106 individuals from three main cities in Germany. Data were collected through surveys that were designed to measure consumers' trust in companies, their personal beliefs on the issue of privacy, and their awareness of German legislating Internet privacy laws.

The results showed that respondents had strong feelings about protecting their privacy (mean = 3.64)

(Singh & Hill, 2003, p. 641). They also agreed that the government and organizations should be involved in protecting the consumers' privacy (Singh & Hill, 2003, p. 641). The respondents said that companies should get permission from consumers before disclosing their information and that violation penalties should be imposed on companies who fail to do so (Singh & Hill, 2003, p. 641). The respondents also suggested that their privacy concerns was affecting their purchase behaviors on the Internet (Singh & Hill, 2003, p. 646). If laws were more effective in protecting consumers' privacy then the consumers would use the Internet more often to make purchases. The researchers noted that "higher levels of expertise should limit concerns about the Internet and not affect actual purchase behavior negatively" (p. 646). The findings of this study suggest that German consumers are homogenous in their opinions about protecting their privacy (Singh & Hill, 2003, p. 642). No statistical differences were noted to relate privacy attitudes and demographic variables.

Similarly, Ackerman, Cranor, and Reagle (1999) studied the perspectives of consumers towards privacy. Their purpose was to find out which information the customers consider sensitive, how customers would respond

to specific situations, and the relationships between demographic variables and attitudes towards privacy (Ackerman et al., 1999, p. 2). The population included 405 US citizens, 88 Canadian citizens, and 30 individuals from other countries.

The results of the survey showed that the consumers were very concerned about their privacy and Internet (Ackerman et al., 1999, p. 2). When the respondents were asked which of the 12 information items given were willing to disclose in specific online situations, the majority of them indicated that they were most comfortable disclosing information about their favorite television show, snack food, email address, and age (Ackerman et al., 1999, p. 3). Very few respondents indicated that they were willing to disclose information about their health, income, and phone number, and none of them was comfortable providing their credit card number and social security number (Ackerman et al., 1999, p. 3).

One question asked the respondents, if they could configure their web browser to find privacy policies on line, what would be the most important factor for them? The respondents indicated the following in order of importance: the sharing of their information with other companies, "whether information is used in an identifiable

way", "the kind of information collected", and the purpose for which information is collected" (Ackerman et al., 1999, p. 4). Lastly, the results showed that posting a privacy policy on line does not mean a lot to consumers (Ackerman et al., 1999, p. 4). The study did not find strong relationships between privacy issues and demographic variables.

Privacy versus Customer Relationship Management

Kakalik and Wright (1996) address the issue of privacy as a concern that should lead to a proactive, and not a reactive approach by organizations (p. 3). Even though, the collection of consumer data is valuable to organizations that want to achieve one-on-one relationships with their customers, it is also a good reason for consumers to view it as a threat to their privacy (Kakalik & Wright, 1996, p. 2). Some examples include the U.S. Postal Services, Credit bureaus, Medical Information Bureau, Federal Parent Locator Service, State Directory of New Hires and Credit Cards are just a few databases that contain consumers' information (Kakalik & Wright, 1996, p. 2). These databases play a role to the dissemination of information, and contribute to the fact that an "average consumer is on more than 100 mailing

lists and in at least 50 databases" (Kakalik & Wright, 1996, p. 16).

For better management, Kakalik and Wright (1996) recommend a three step proactive approach to any future predicaments with legal privacy issues. The first step is to "accept greater responsibility for consumer data" (p. 3) particularly, when retrieving and using a client's information (Kakalik & Wright, 1996, p. 4). The second step is to "establish a collaborative philosophy" (Kakalik & Wright, 1996, p. 3) that will lead to fewer misunderstandings (Kakalik & Wright, 1996, p. 6). The third step is to "enact proper standards of behavior" (Kakalik & Wright, 1996, p. 3) by providing customers with benefits that make it reasonable for them to give out their information (Kakalik & Wright, 1996, p. 6).

Hubbell and Redding (2003) attach importance to the positive outcomes of such advances, especially in the financial services organizations because of the need to understand better their customers (p. 45). Some of the benefits of CRM include predictions of customers' preferences, investments at individual customer level, allocations of marketing, sales and service resources, measurement of the effectiveness of resource allocation

decisions, and intelligent decision-making (Hubbell & Redding, 2003, p. 46)

However, they make clear that if financial organizations do not put any efforts into creating trust between them and their customers, then the customers will become more cynical when they will be asked to give out their information (Hubbell & Redding, 2003, p. 49).

Likewise, Aldhizer and Cashell (2004) nod to the fact that CRM-DMS (Customer Relationship Management and Data Management Systems) produce concerns about unauthorized access and security in databases (p. 54). These risks are not only harmful for the customers, but for the company itself (Aldhizer & Cashell, 2004, p. 55). For example, unauthorized users may steal important data and sell it to competitors or make illegal changes that will ultimately harm the organization (Aldhizer & Cashell, 2004, p. 55). Also, with unauthorized access, users make it possible to retrieve customers' personal information and use it for identity theft (Aldhizer & Cashell, 2004, p. 55). Aldhizer and Cashell (2004) acknowledge that CRM-DMS has strong, positive effects on the internal structure and the organization of a company, but also concede the need for security alerts for both the customers and the companies (p. 58).

Similarly, Pitta, Franzak, and Laric (2003) note the most important dynamic between CRM and privacy is trust (Pitta et al., 2003, p. 627). They explain that incidents like consumer fraud, identity theft, and "the deceptive use of 'consumer surveys' as selling techniques" generate alerts in consumers' minds (Pitta et al., 2003, p. 616). Companies that want to maintain long-term relationships with their customers need to create a reciprocal relationship (Pitta et al., 2003, p. 624) and suggest a three-tiered approach. The first step for the company is to collect enough information to be able to find their customers (Pitta et al., 2003, p. 623). The second step includes the analysis of the information to turn it into valuable knowledge about the customers (Pitta et al., 2003, p. 624). The final step is for the business to actually meet the customers' needs (Pitta et al., 2003, p. 624).

Long, Hogg, Hartley and Angold (1999) examined the thresholds of consumers when companies collect and use their personal information. The researchers used Zaichkowsky's Personal Involvement Inventory Scale (PII) to measure the levels of involvement of the participants and found that there are "different thresholds of involvement in relation to information privacy" (Long et

al., 1999, p. 9). Further findings showed that respondents "were very skeptical about the amount of information which was requested by companies" unless "they were going to benefit from completing the application form" (Long et al., 1999, p. 10). Also, responses in this stage revealed that participants were very sensitive in passing out their financial information and telephone numbers, but were more open in disclosing information about their attitudes (Long et al., 1999, p. 12).

When participants were asked whether they were willing to disclose information where they would receive benefits, they showed positive attitudes suggesting equality in the relationship (Long et al., 1999, p. 12). They also found that the respondents expressed that they desired free and complete access to their records (Long et al., 1999, p. 13).

Finally, when asked to put in order the types of companies that they felt more comfortable disclosing information to respondents indicated the following: utility companies, travel and leisure, department stores, high street retailers and supermarket, and do-it-yourself and electrical stores (Long et al., 1999, p. 15).

Radio Frequency Identification

Radio Frequency Identification (RFID) applications were first used in World War II for military purposes, and in the 1980s for commercial purposes (i.e. for highway tolls in USA, Italy, France, Portugal and Norway) (Jones, Clarke-Hill, Comfort, Hillier, & Shears, 2005, p. 356). Since then, numerous studies have been conducted to explain the importance of RFID applications for businesses: in food retailing (Jones et al., 2005), in supply chain facilities (Twist, 2005), and airline operations (Wyld et al., 2005). On the contrary, few studies have been conducted to measure the perception of consumers regarding RFID, possibly because it is a widespread technology within organizations, which consumers are not aware of.

Cohen (2004) indicates concerns that come along with the loss of privacy and the advancements in technology. He refers to RFID (Radio Frequency Identification), TIA (Total Information Awareness), and location-tracking cell phones as some of the most recent technologies that are becoming threats to privacy (Cohen, 2004, p. 130) for consumers. He raises such questions as "Can someone find out enough about me to steal my identity and get me in all sorts of trouble?" and "What privacy safeguards are out

there to protect me?" (Cohen, 2004, p. 129). As a referral to the second question Cohen (2004) argues that "privacy is often taken for granted as an inherent right of every citizen, but in fact the U.S. has one of the weakest privacy protection schemes in the developed world" (p. 130). "The European Union, Canada and Japan all trump us in terms of privacy" (Cohen, 2004, p. 130). He notes that "the average American is in at least 50 databases… and that's just counting commercial databases" (Cohen, 2004, p. 131). Being a self-regulatory industry, organizations are realizing that without adequate privacy policies profits will drop (Cohen, 2004, p. 132) and with more security and protection, the more likely customers will create a sense of trust with businesses (Cohen, 2004, p. 132).

Gunther and Spiekermann (2005) examined the perceptions of 129 German customers relating to privacy issues instigated by RFID (Gunther & Spiekermann, 2005, p. 73) and found that "regardless of PET [privacy enhancing technologies] employed, consumers felt helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be" (Gunther & Spiekermann, 2005, p. 75). Findings showed that customers

would have difficulty accepting and trusting the RFID technology.

While Gunther and Spiekermann (2005) examined only the attitudes of customers on RFID, Juban and Wyld (2004) took into consideration the perceptions of both the customers and the organizations regarding RFID and examined perceptions of these groups regarding RFID. The first survey among consumers found that only 23% of them were aware of the RFID technology (Juban & Wyld, 2004, p. 35). Of that 23%, 42% expressed their favoritism, and only 10% expressed adverse feelings towards RFID (Juban & Wyld, 2004, p. 35). The survey concluded that the five most important benefits of RFID as listed by the participants are: "faster recovery of stolen items", "improved car anti-theft capabilities", "consumer savings due to decreases in manufacturing and retail costs", "improved security of prescription drugs" and "faster, more reliable recalls and improved food safety/quality" (Juban & Wyld, 2004, p. 35).

On the other hand, consumers ranked the following concerns of RFID: "consumer data used by third party", "targeted more with direct marketing", "tracking of consumers' purchases", "health issues stemming from RFID", "environmental impact", "RFID tags can be

eaten/dissolved", "tags could be read from a distance" (Juban & Wyld, 2004, p. 36). When respondents were asked whether they would buy products from a retailer that uses RFID tags and monitors the consumers payment information "29% said they would definitely buy, 26% said they might buy and 45% said they would definitely not buy at all" (Juban & Wyld, 2004, p. 36).

Juban and Wyld (2004) conducted another survey among users and developers of RFID systems and found that developers forecasted that RFID would affect pallet tracking, item tracking and asset management. In addition, they predicted that the industries that would use RFID the most were retail, manufacturing, transportation and automotive (Juban & Wyld, 2004, p. 36). Only 33% of users said that security was a valuable asset for the success of RFID (Juban & Wyld, 2004, p. 36). Users also ranked the following as benefits that RFID will bring to their organizations: "trailer/container tracking", work-in-progress tracking", and "item level tracking" (Juban & Wyld, 2004, p. 37).

The main difference between the two was surveys: the knowledge level of the participants regarding RFID (Juban & Wyld, 2004, p. 38). The TRA model argues that consumers' attitudes towards technology change based on their peers'

attitudes. In the first survey, participants knew little or nothing about RFID, meaning that those participants would spread a negative attitude to their peers due to their lack of knowledge (Juban & Wyld, 2004, p. 38). Both the TRA model and the Innovation Diffusion Theory agree on the fact that unawareness can delay the adoption of the technology (Juban & Wyld, 2004, p. 38). Juban and Wyld (2004) suggest that the TAM model is more appropriate because it gives an explanation of how technology becomes accepted even when there is little information about it (Juban & Wyld, 2004, p. 38). The authors assent that TAM is more appropriate because "the two key variables to the model, perceived usefulness and ease of use, impact attitudes for both experienced and novice users" (p. 38). Moreover, they imply that RFID will benefit organizations more than customers because organizations spend millions of dollars on a daily basis (Juban & Wyld, 2004, p. 38).

With a different approach, Eckfeldt (2005) identifies the myriad of privacy problems that RFID systems will instigate once they become a part of a consumer's everyday life. He acknowledges the fact that some RFID systems have been welcomed by the public in the United States (i.e. highway toll payment systems) because in those cases the benefits overshadow the privacy issues (Eckfeldt, 2005,

p. 78). Eckfelt (2005) notes that a balanced equation between consumers' and companies' point of view can lead an RFID application to success (Eckfeldt, 2005, p. 78). Yet he makes his distrust to companies clear by saying they companies should not "benefit solely from their own self-centered points of view, which are inherently biased in favor of the technology and its derivative uses due to their greater understanding of and experience with RFID, along with their own selfish business interests" (Eckfeldt, 2005, p. 78).

However, Eckfeldt (2005) suggests two basic solutions to companies: 1) decreasing the privacy risks of consumers by educating the public and creating privacy policies, and 2) increasing the benefits for consumers such as lower prices, faster checkouts, and more convenient shopping (Eckfeldt, 2005, p. 78).

Summary of Literature Review

CRM promotes one-to-one personalized relationships between companies and their customers. The intention of CRM is to target individuals and meet their demands, while it creates loyalty that will eventually bring long-term profits to the company.

It is hard to disagree on the strengths of CRM, but the controversy begins with a look at the technical part of it. CRM is made possible with the help of data mining technology, which allows companies to create detailed profiles on their customers. These kinds of profiles are essential for CRM strategies. They are extremely useful when a company attempts to target a customer on a personalized level. Even though the tailoring of services characterizes the strength of CRM, many scholars (Kakalik et al., 1996; Cohen, 2004; Hubbell et al., 2003) argue that it also instigates concerns about privacy. The creation of detailed customer profiles and the ability to be transferred and viewed by many companies worldwide create apprehension about the technological innovations that lie behind CRM. Hence, privacy becomes the main focus with CRM.

By building an equal relationship whereby both the organization gets information and the customer gets benefits will CRM boost company profits. As far a as privacy and security are concerned, the information must be foremost in the company to hold a trusting, ongoing relationship with the customer.

Nevertheless, scholarly research lacks in providing information on customers' perceptions on privacy, and then

correlating it to customers' demographics. It is clear through this Literature Review that more research needs to be conducted in order to strengthen the results we have so far on CRM and privacy perceptions.

More research has been conducted regarding RFID and the way consumers perceive its uses. Research suggests that consumers have very little knowledge regarding the applications of RFID. Previous studies found that consumers reject the uses of RFID that intrude their personal lives.

CHAPTER THREE

METHODOLOGY

Population

The population of the study was students enrolled in a southwestern university. The researcher chose a convenience sample of 203 students from two business classes (one graduate and one undergraduate), and one psychology undergraduate class. With the permission of professors and students, questionnaires were completed during their classes. An informed consent form was attached to the survey explaining to the participants the study was about consumer attitudes towards privacy issues.

Instrument Development

Question 1 was created based on the instrument developed by Ackerman, Cranor and Reagle (1999). The researchers asked participants to rate the level of importance (using three levels: very important, somewhat important, or not important) of ten criteria when they visit a web site (Ackerman et al., 1999, p. 4). The most important criteria cited included: "sharing of information with other organizations", "whether information is used in an identifiable way", "the kind of information collected",

and "the purpose for which the information is collected" (Ackerman et al., 1999, p. 4).

For the present study, a modified five-point Likert type scale was used to measure the importance of the 18 criteria when conducting business with organizations (see Appentix A). These criteria were: protecting the privacy of my information, good customer service, product service satisfaction, cost of product/ service, personalized relationship, mutual trust, knowledgeable staff, accessibility i.e. web site, call centers, availability (extensive customer service hours), the option to opt in or opt out when asked to disclose personal information, selection of merchandise/services, feedback on requests, complaints, suggestions, convenient shopping, frequent buyer reward program, fast problem resolution, compensation/rewards for inconvenience, tailored services based on the individual needs and demands, and human-to-human interaction.

A focus group was conducted to obtain exploratory data regarding what is considered private information. The focus group was asked to list information items that they consider being private. Based on the responses of the focus group a list of twenty-six information items was created and used in Questions 2 and 3 of the instrument.

This information included: social security number, employer, e-mail address, credit card number, telephone number, occupation, annual income, ethnicity, mailing address, owned assets, owned investments, place of birth, date of birth, legal history, mother's maiden name, health related information, gender, number of children, sexual orientation, home expenses, work telephone number, wireless telephone number, driver's license/ID number, citizenship, passport number, places lived.

A modified Likert scale was also used to measure the willingness of the participants to disclose private information. They were given 26 information items that were collected from a prior focus group. The scale gave participants five options to choose from regarding privacy for each item: 1) Definitely Private and always protected; I would not share with businesses, 2) Somewhat Private; share with family and friends, and used in normal transactions, 3) Indifferent, 4) Private, but willing to share occasionally and on a limited basis only, and 5) Private, but less hesitant to share with organizations I conduct business with.

White (2004) used a similar method to determine what kind of information consumers were willing to disclose in shallow vs. deep relationships (p. 45). The researcher

provided the participants only four information items that were separated in two categories: privacy-related information and embarrassing information (White, 2004, p. 45). This information provided a foundation for the issues and responses presented in question two of the present study.

For the next question participants were given four scenarios and were asked to indicate which ones (if any) they have experienced in the last twelve months. This section was based on a modified version of the Ackerman et al. (1999) instrument was used.

In the present study participants were given four scenarios. Additionally, 26 information items employed in question 2 were included. Participants were asked to indicate what information they were willing to disclose during each scenario-transaction that they have experienced in the last twelve months. Two of the scenarios included a high and a low involvement purchase of a product (Scenario #1 and Scenario #4 respectively). Specifically, Scenario #1 was about a purchase of car from a dealership, and Scenario #4 was about the use of a credit card to purchase appliances or electronics. The other two scenarios included a high and a low involvement purchase of a service (Scenario #2 and Scenario #3

respectively). Scenario #2 was a purchase of Auto Insurance and Scenario #3 was an on-line hotel reservation.

In question four a Likert scale (ranging from 1 strongly disagree to 5 strongly disagree) was used to measure statements regarding privacy that included awareness, knowledge and attitudes. The Singh and Hill (2003) instrument regarding privacy attitudes was used in the present study.

Question five asked the participants whether they were aware of RFID technologies. This was measured using a yes or no response. Following this question a definition of RFID technologies was given.

The next section used a modified Likert scale ranging from 1 to 5 to measure the level of acceptance of selected uses of RFID in Business. The instrument developed by Gunther and Spiekerman (2005) was modified and employed in the present study to include 11 benefits of RFID.

Demographic variables were also measured and were retrieved from the literature reviewed. Data were analyzed using measures of central tendency and cross tabulations.

CHAPTER FOUR

RESULTS

Data Analysis

This study examined the relationships between demographic variables and attitudes towards privacy. Data was collected among 203 students at a southwestern university. Descriptive statistics were used to identify the mean value of the variables for all questions. Also, cross tabulations were applied to examine the relationships between the demographic variables and the customers' attitudes towards privacy issues.

Description of Respondents

The total number of participants was 203 of which 72.6% of them were female (see Table 1). The majority were aged between 18-24 (60.1%) and had some college experience (72.1%). Most respondents were white (43.6%), followed by Hispanics (32.8%). Data were divided into 3 groups based on the class during which they completed the survey: undergraduate students in a business class, graduate students in a business class, and undergraduate students in a psychology class (see Table 2).

The first question asked the respondents to rate the importance of 18 criteria when conducting business with organizations.

Table 2. Sample Demographics

Demographics	Percentage %
Gender:	
Male	27.4
Female	72.6
Age Group:	
18-24	60.1
25-36	28.8
37-48	5.1
49-64	6.1
Highest Level of Education:	
Some High School	1.0
High School Graduate	1.5
Some College	72.1
Graduated College	21.8
Post Graduate	3.6
Race/Ethnicity:	
White	43.6
Black	6.2
American Indian	1.0
Asian/Middle Eastern	12.3
Hispanic	32.8
Other	4.1
Data Collection:	
Business Undergraduate students	35.5
Business Graduate students	6.9
Psychology Undergraduate students	57.6

Source: Retrieved from current study.

Participants were given a 5-point modified Likert scale rating from 1 being very unimportant to 5 being very

important. The most important was "cost of product/service" (4.61) (see Table 3). Criteria that were rated least important were "Frequent Buyer Reward program" (3.39), "Tailored services" (3.74), and "Personalized Relationships" (3.40) (see Table 3). These responses indicated that participants were indifferent about those criteria. It is likely that the participants were not familiar with the terms. Responses did not vary across demographic variables.

Regarding the second question, participants were asked to indicate their willingness to disclose 26 select information items. Social security number and Passport number were the only two information items with a mean value of 1.82 and 1.90 respectively. These responses show that participants considered their social security number and their passport number to be the most private and protected. Participants felt indifferent for information like ethnicity, gender, sexual orientation, citizenship, number of children, and employer (see Table 4).

Table 3. Highest Mean Values of Criteria when Conducting Business with Organizations

Variable:	1 %	2 %	3 %	4 %	5 %	Mean
Cost of product/service	5.9	3.9	7.9	31.0	49.8	4.61
Protecting the privacy of my information	9.4	0.5	2.0	8.4	79.8	4.49
Product/service satisfaction	8.9	1.5	3.0	11.8	74.4	4.42
Good Customer Service	7.9	2.5	3.0	14.8	71.9	4.40
Knowledgeable staff	6.9	3.4	6.9	24.6	57.6	4.23
Fast problem resolution	7.4	5.9	7.9	23.6	55.2	4.13
Mutual Trust	6.9	3.0	9.9	34.5	43.8	4.08
Selection of merchandise services	5.4	6.4	5.9	40.9	40.4	4.05
Human-to-human interaction	5.9	10.8	16.3	30.5	36.5	4.03
Convenient shopping	4.4	8.9	9.4	34.5	42.9	4.02
The option to opt in or opt out	8.9	3.9	12.8	26.6	47.3	4.00
Accessibility	6.9	5.4	12.3	36.5	38.9	3.95
Availability	6.9	4.4	15.3	38.4	35.0	3.90
Compensation/ rewards	6.9	7.4	14.3	37.4	33.0	3.83
Feedback	5.4	10.3	16.7	33.0	34.5	3.81
Tailored services	4.4	8.9	20.2	40.4	25.6	3.74
Personalized Relationship	4.9	13.3	34.5	31.0	15.8	3.40
Frequent Buyer Reward Program	5.9	15.8	32.5	24.6	20.7	3.39

Source: Retrieved from current study.

Table 4. Consumers' Willingness to Disclose Personal Information; in Order of Highest Mean Values

Variables	1 %	2 %	3 %	4 %	5 %	Mean
Social Security Number	65.0	14.8	0.5	10.8	8.4	1.82
Passport number	59.6	14.8	10.8	4.4	9.9	1.90
Credit Card Number	49.8	24.6	2.0	11.3	11.8	2.10
Health related information	37.4	28.1	19.7	8.4	5.9	2.17
Owned Investments	42.9	19.2	18.7	7.9	9.9	2.22
Legal History	6.9	10.3	47.8	12.8	21.2	2.24
Owned Assets	36.0	28.1	18.2	7.4	9.4	2.25
Driver's Livense/ID number	42.4	25.1	5.9	14.3	11.8	2.28
Mother's maiden name	31.7	27.2	22.8	8.9	9.4	2.37
Wireless telephone Number	25.6	37.4	10.3	15.3	10.8	2.48
Home expenses	22.8	28.2	28.7	11.9	8.4	2.55
Home Telephone Number	17.2	36.5	16.7	19.7	9.4	2.67
Annual Income	21.7	24.6	25.1	16.7	10.3	2.69
Work Phone number	17.8	34.7	19.8	14.9	12.9	2.70
Mailing Address	8.4	42.4	15.3	22.2	11.3	2.86
Places lived	11.4	24.9	39.3	13.4	10.9	2.88
Date of birth	9.4	22.3	39.1	13.4	15.8	3.04
Sexual Orientation	15.5	11.0	46.5	8.5	18.5	3.04
Email address	4.4	38.4	21.2	17.7	17.9	3.05
Number of children	8.9	15.3	50.0	11.4	14.4	3.07
Place of birth	9.9	19.3	40.6	12.9	17.3	3.08
Occupation	4.5	21.8	39.1	15.3	19.3	3.23
Employer	5.0	18.8	42.1	14.4	19.8	3.25
Ethnicity	6.9	10.3	47.8	12.8	21.2	3.31
Citizenship	8.5	10.0	48.3	9.0	24.4	3.31
Gender	5.4	11.4	52.0	7.4	23.8	3.33

Source: Retrieved from current study.

In question 3a respondents were asked to indicate which of the four scenario-transactions (if any) they experienced in the last twelve months. Approximately, 25% indicated that they bought a car, 27.8% indicated that they bought auto insurance, 38.9% indicated that they made an on-line reservation for a hotel, and 52.5% indicated that they made a credit card purchase of electronics.

Following this, respondents were asked of the 26 select information items they were willing to disclose during each of the four scenarios. Findings showed that the majority of participants were more willing to disclose information when buying a car from a dealership such as: mailing address, home telephone number, employer, occupation, driver's license/id number, annual income, and social security number (see Table 5). These responses were not found to vary across demographic variables.

Table 5. Percentages and Mode Values for Scenario-transaction #1 (Buying a Car from a Dealership)

Information item:	Yes 1	No 0	Mode
	%	%	
Mailing address	83.0	17.0	1
Home Telephone Number	81.0	19.0	1
Employer	81.0	19.0	1
Occupation	78.9	21.1	1
Driver's License/ID Number	76.9	23.1	1
Annual Income	75.5	24.5	1
Social Security Number	72.1	27.9	1
Date of birth	68.0	32.0	1
Work telephone number	60.5	39.5	1
Gender	57.1	42.9	1
Wireless telephone number	55.8	44.2	1

Source: Retrieved from current study

The second scenario, which was also a high involvement service purchase buying auto insurance, participants indicated that they were most willing to disclose their home telephone number, employer, and gender (see Table 6).

Table 6. Percentages and Mean Values for Scenario-transaction #2 (Buying Auto Insurance)

Information Item	Yes 1	No 0	Mode
	%	%	
Mailing address	85.2	14.1	1
Home Telephone Number	84.4	15.6	1
Driver's license/ID number	76.9	23.1	1
Date of birth	68.1	31.9	1
Occupation	67.4	32.6	1
Gender	63.3	36.3	1
Employer	57.8	42.2	1
Wireless telephone number	54.8	45.2	1
Social Security	51.9	48.1	1
Work telephone number	51.1	48.9	1

Source: Retrieved from current study.

For making hotel reservations on line (a low involvement purchase of service) respondents indicated that they were most willing to disclose the following information: credit card number, home telephone number, email and mailing address (see Table 7).

Table 7. Percentages and Mean Values for Scenario-transaction #3 (Making On-line Reservations for a Hotel)

Information Item	Yes #1	No #0	Mode
	%	%	
Email Address	79.2	20.8	1
Credit Card Number	82.5	17.5	1
Home Telephone Number	75.0	25.0	1
Mailing address	74.3	25.7	1

Source: Retrieved from current survey.

For the last scenario, making a credit card purchase of electronics, the majority of respondents (82.6%) indicated that they were most willing to disclose their credit card number (see Table 8).

Question 4 asked respondents to use a 5-point Likert scale to show their agreement or disagreement with 18 privacy statements. The statement "I consider invasion of privacy to be the use of my personal information without my consent" had the highest mean value (4.39).

Table 8. Percentages and Mean Values for Scenario-transaction #4 (Making a Credit Card Purchase of Electronics)

Information Item	Yes #1 %	No #0 %	Mode
Credit Card Number	82.6	16.8	1
Home Telephone number	61.7	38.3	1
Mailing address	71.8	28.2	1

Source: Retrieved from current study.

For the rest of the statements most of the responses varied between "indifferent" and "agree" (see Table 9). Responses did not vary across demographic variables.

In question, 5, respondents were asked of their knowledge of RFID technologies. Even though none of the demographic variables played any role in the awareness of RFID technologies, there were some distinctions made between graduate students from the business class and undergraduate students from a business and psychology class. Graduate students from a business class had the highest percentage (35.7%) of awareness (see Table 10).

Table 9. Percentages and Mean Values for Privacy Statements

Privacy Statements	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Mean
	#1 %	#2 %	#3 %	#4 %	#5 %	
Invasion of privacy is the use of my information without my consent	2.0	3.0	7.0	30.2	57.3	4.39
I am aware of the risks when I disclose personal information	4.5	9.1	8.1	48.5	29.8	3.90
I am always afraid to give information over the phone	1.5	15.6	14.6	35.2	33.2	3.83
I disclose personal information to companies I trust	2.5	11.1	15.2	44.4	26.8	3.82
I am always afraid to give information on the internet	2.5	15.2	19.7	34.8	27.3	3.71
I feel unsafe with today's environment	4.2	9.4	26.6	33.9	24.5	3.64
My privacy concerns influence my purchase behaviors	5.0	10.1	30.2	34.2	20.1	3.56
I am worrying about my finances	5.5	24.6	17.6	38.2	14.1	3.31
I feel that I am monitored by companies	6.1	17.7	30.8	30.3	15.2	3.31
I always make sure that my information not shared with third parties	7.5	24.1	15.1	37.2	15.6	3.31
I always look for the privacy policy	8.5	23.1	21.1	29.6	17.6	3.25
I feel that I lost control over my privacy	7.0	29.1	27.1	23.1	13.6	3.07
I read carefully the privacy notices	12.1	29.1	14.6	33.7	10.6	3.02
As a consumer I am aware of all the legal protections I have	9.5	35.7	21.6	23.1	10.1	2.88

Source: Retrieved from current study.

Table 10. Frequencies for Radio Frequency Identification Awareness

		Business Undergraduate students	Business Graduate students	Psychology Undergraduate students
Have you ever heard of RFID?	Yes %	18.6	35.7	8.0
	No %	81.4	64.3	92.0

Source: Retrieved from current study.

Regarding responses on statements about RFID uses, all three classes of respondents agreed on statements regarding RFID tags as solutions to prevent theft or fraud in retail, the pharmaceutical industry, and for supply chain management (see Table 11). All respondents felt strongly about using RFID tags to prevent theft in stores. Very few respondents found the use to be unacceptable. Regarding the statement to prevent counterfeit medication, the undergraduate students showed a variety of responses (the majority found the use to be acceptable), where as the graduate respondents felt strongly about accepting the use. Even though the use of RFID tags in supply chain management gained the acceptance from the majority of the respondents, a few undergraduate respondents felt indifferent about the use.

Table 11. Responses for Radio Frequency Identification Uses

Statements	Business Undergraduates			Psychology Undergraduates			Business Graduates		
	VA	I	VU	VA	I	VU	VA	I	VU
	%			%			%		
As tags on merchandise to prevent theft	50.7	9.9	7.0	54.5	7.3	7.3	57.1	7.1	0
As tags in drugs to prevent counterfeit medications	25.4	6.9	14.1	42.9	0	7.1	23.6	19.1	12.7
As tags implanted on merchandise for safe transfer within supply chain	32.9	18.6	5.7	42.9	0	0	27.3	17.3	6.4
As tags on store items that are deactivated at the point of sale	52.1	9.9	7.0	50.0	0	0	48.2	8.2	7.3
As tags on prescribed medications to insure proper dispersion by the pharmacist	19.7	26.8	8.5	50.0	7.1	0	21.3	25.9	10.2
As tags implanted in products to return stolen or lost products to their owners	25.4	16.9	5.6	42.9	0	0	20.9 9.1	10.9	

Source: Retrieved from present study

The majority of respondents favored the use of RFID as tags deactivated at the point of sale. Psychology students found it to be very acceptable followed by business undergraduates, and business graduates. Psychology students were rather indifferent about the use

of RFID tags on medications to insure proper dispersion by the pharmacist; where as the graduate respondents were least indifferent.

All the respondents felt strongly against the use of RFID tags implanted in humans to increase access control. Specifically, regarding "RFID tags can be implanted in humans to increase access control to computer systems, medical records, building etc" the majority of the psychology undergraduate respondents (65.5%) found the use to be very unacceptable. "Very unacceptable" was also the most common response from the business undergraduate respondents (50.7%). Business graduate respondents were split regarding their responses.

For the remainder of the statements graduate and undergraduate respondents responded differently. The graduate respondents seemed to be more open-minded about the uses of RFID to gather information from customers or products and transmit it to vendors for marketing purposes or for discounts. Undergraduate respondents from both classes opposed to these statements by finding them very unacceptable (see Table 12).

Table 12. Differences in Responses for Radio Frequency Identification Uses

Statements	Business Undergraduates			Psychology Undergraduates			Business Graduates		
	VA	I	VU	VA	I	VU	VA	I	VU
	%			%			%		
As tags to gather information about the product	7.0	14.1	35.2	35.7	0	0	7.3	14.5	47.3
As tags in drugs to insure compliance by the patient	12.7	15.5	15.5	42.9	7.1	0	10.0	18.2	24.5
As tags on products to transmit information about the customer	7.0	11.3	59.2	35.7	14.3	21.4	8.2	9.1	69.1
As tags on products that will provide discounts to customers	9.9	39.4	12.7	28.6	21.4	7.1	9.1	23.6	25.5

Source: Retrieved from current study.

Regarding the statement: "As tags implanted in products to gather information after the purchase on product image, location and use, and transmit it to vendors". The two most common responses from graduate students were "Very Acceptable" and "Somewhat Acceptable" with 35.7% in both cases. On the other hand, undergraduate respondents from the business and the psychology classes most commonly stated that it was "Very Unacceptable" (35.2% and 46.4% respectively).

Regarding the statement: "As tags on prescribed medications to identify the user and to insure appropriate

compliance by the patient", the most common response from graduate students (42.9%) indicated that it is "Very Acceptable". While undergraduate students from the psychology class found acceptable the use of RFID as tags on medications to insure proper dispersion from pharmacists, they also found it unacceptable its use to monitor patients' compliance with the instructions. The most common response by undergraduate students from the psychology class was "Somewhat Unacceptable" (30.9%). Undergraduate business students split their answers between "Somewhat Acceptable" and "Somewhat Unacceptable" (28.2%).

Regarding the statements: "As tags on purchased items that can transmit personal information of the customer to the vendors (i.e. age, address etc) for marketing purposes" graduate respondents showed their favoritism towards the use. Interestingly, while the majority of graduate students (78.6%) indicated in the first question that protecting the privacy of their information was very important to them, their most common response to the above use of RFID was very acceptable (35.7%). Undergraduate students, who had also indicated in the first question that the privacy of their information was very important (Business undergraduate students = 83.3%, Psychology

undergraduate students = 77.8%), also indicated that it was "Very Unacceptable" to use RFID tags to transmit customers' private information to companies (Business undergraduate students = 59.2%, Psychology undergraduate students = 69.1%).

Regarding the RFID statement: "As tags on products that will provide discounts and special offers to customers who choose not to deactivate them at the point of sale", graduate students found the use to be somewhat acceptable, whereas undergraduate students had varying responses.

Discussion

The present study sought to determine the influence of demographic characteristics on individuals attitudes toward privacy. Questions were designed to measure participants' awareness, knowledge, and attitudes towards privacy. In addition, participants were asked to show their willingness to disclose certain information items during selected scenario-transactions. Moreover, the study examined the acceptance level of individuals for possible RFID uses.

Findings showed that educational level respondents played a role in the way they perceived the uses of RFID.

Graduate students were more open-minded in accepting the applications of RFID, as opposed to undergraduate students who were more undecided.

Protecting the Privacy of My Information

Although, the graduate students indicated that they were more open-minded about disclosing private information through the uses of RFID, 78% of them also indicated that protecting the privacy of their information was very important. Similar results were also found in the study by Graeff and Harmon (2002) that suggested inconsistency among respondents by the responses of high income.

Findings also showed that "protecting the privacy of my information" was the most important criterion for the majority of the respondents (79.8%) when they conducted business with an organization. In addition, 53.3% of the respondents agreed or strongly agreed with the statement "I always make sure that my personal information will not be shared with third parties". As well, Singh and Hill (2003) found that respondents felt strongly about protecting their privacy. However, Ackerman et al. (1999) found that 96% of the respondents "rated the sharing of their information with other companies and organizations as the most important factor" for having configured their web browser to search for privacy policies (p. 4).

Trust

Findings showed that respondents prefer to disclose personal information only to companies they trust (71.2%). Moreover, 79.9% of the participants indicated that "mutual" trust is somewhat important or very important criterion when they conduct business with a company. Ackerman et al. (1999) also found that 69% of the respondents indicated that it was very important to know whether a site was operated by a reputable organization" (p. 4). "The option to opt in or opt out when asked to disclose personal information" was found to be important by 74.2% of participants of the present study. Similarly, the respondents in the study by Ackerman et al. (1999) found that "whether the site will remove someone from their mailing lists upon request" was a very important factor to consumers (p. 4).

Similarly, concurrent to Ackerman et al. (1999) fewer respondents agreed with the statement "I read carefully the privacy notices I receive from companies I do business with" (44.3%). These concurring results suggest that customers do not take the time to read the privacy policies possibly because they are very extensive or as Ackerman et al. (1999) suggest "it is not enough for

people to know that a privacy policy is present - it is more important to know what the policy states" (p. 4).

Sensitive Information

Similar to the results of the study by Ackerman et al. (1999), respondents of the present study showed that they were more sensitive about disclosing certain information. For example, Ackerman et al. (1999) found that only 18% felt comfortable disclosing health related information (p. 3). The present study also found that only 5.9% of the participants were less hesitant to disclose health related information with companies they conduct business with. Also, concurrent with Ackerman (1999) only a few respondents indicated that they were less hesitant in giving out their credit card number. Finally, findings indicated that the majority of the participants consider their social security number and passport number to be the most private and should be protected.

Acceptance of Radio Frequency Identification Uses

Among respondents only 13.7% knew about RFID. Similarly, the results of a study by Cap Gemini Ernest and Young (2004) revealed similar findings about the awareness of RFID. Their findings revealed an awareness among 13% of the sample (as cited in Juban & Wyld, 2004, p. 35).

In the present study, whether participants were aware of RFID technologies or not the majority agreed that applications of RFID will help decrease theft and fraud and will not intrude with privacy. For example, the majority of the participants agreed with the statement that RFID tags should be deactivated before the customer leaves the store (77.9%). The study by Gunther and Spiekerman (2005) found similar results in acceptance of RFID uses and invasion of privacy. In their study, 73% agreed that RFID tags should be deactivated before customers leave stores (p. 73). They also noted that 78% of the highly educated consumers agreed with RFID tags being deactivated at the point of sale (p. 74).

In the present study, the majority of the participants also agreed on the following statements:

1. "As tags on merchandise in stores to prevent theft"
2. "As tags in the pharmaceutical industry that are implanted in drugs to prevent counterfeit medications"
3. "As tags implanted on merchandise to insure safe transfer of products within supply chain (will insure that products are properly handled and not stolen)"

4. "As tags on prescribed medications to insure that they are dispersed properly and accurately by the pharmacist", and
5. "As tags implanted in products that can help return stolen or lost products to their owners".

Similar to the present study, Cap Gemini Ernest and Young study found that the most favorable benefits of RFID were(in order of importance): "faster recovery of stolen items", improved anti-theft capabilities", consumer savings due to decreases in manufacturing and retail costs", improved security of prescription drugs", and "faster, more reliable recalls and improved food safety/quality" (as mentioned in Juban & Wyld, 2004, p. 35).

However, given that more graduate students knew about RFID more than undergraduate students (35.7% business graduates, 18.6% business undergraduates, 8.0% psychology undergraduates) their responses towards some of the uses of RFID were different from those of the undergraduate students. This is concurrent with the findings by Cap Gemini Ernest and Young (Juban & Wyld, 2004, p. 36). The present study also found that 76.5% of the participants felt strongly against RFID as tags on products that transmit information about the customers to vendors. The

majority of the participants who rejected this application were undergraduate students (62.8%).

The findings suggest that the graduate students from a business class were more liberal in accepting the possible uses of RFID that could initiate privacy concerns. For instance, graduate and undergraduate students disagreed on the use of RFID "as tags on purchased items that can transmit personal information of the customer to the vendors (i.e. age, address) for marketing purposes. Even though the majority of the participants did not accept this application, graduate students were more in favor of such an application than undergraduate students. On the contrary, graduate students felt that using RFID to transmit customer information to marketers was acceptable (64.3%). As found in the present study Ackerman et al. (1999) found that many consumers don't understand this technology and therefore find it an invasion of privacy (p. 4).

The other uses of RFID that graduate students were in favor of and undergraduate students did not support are:

1. "As tags that are implanted in products to gather information after the purchase on product image, location and use, and transmit it to vendors",

2. "As tags on prescribed medications to identify the user and to insure appropriate compliance of the instructions by the patient", and
3. "As tags on products that will provide discounts and special offers to customers who choose not to deactivate them at the point of sale".

Given that graduate students are exposed to new technologies and perhaps through work experience, their attitudes towards this technology maybe more favorable than those of undergraduates.

CHAPTER FIVE

SUMMARY, CONCLUSIONS, AND IMPLICATIONS

Summary

George Orwell's description of a society without any privacy boundaries seems to becoming a reality only a few decades after his foretelling. Privacy concerns are now the focal point of research in recent years with extensive work conducted related to consumers' concerns with Customer Relationship Management and RFID technologies. Such innovations are being used by governments for security reasons and by organizations to better market to their target audience. Previous research (Fletcher, 2003; Gunther & Spiekerman, 2005; Graeff & Harmon, 2002) suggests that there is an increasing finding of apprehension among individuals about the way their information is being used by organizations and the government. Moreover, their concern is amplified by the ramifications of that loss of privacy on their lives.

Scholars (Evans, 2003; Cannon, 2002) condemned the employment of CRM strategies, while others have expressed positive attitudes (Hubbell & Redding, 2003) towards its outcomes. Furthermore, issues of trust and loyalty were also found to be important aspects in the compromise of

CRM and privacy conflict (Kavali et al., 1999; Grossman, 1998).

The purpose of this study was to determine the relationships between demographic variables and individuals' attitudes towards privacy. A quantitative research was conducted at a southwestern university and a convenience sample of 203 graduate and undergraduate students was used. The data was collected from two business classes and one psychology class. The data were analyzed using central tendency and cross tabulations. Results from the study indicate that educational background played a role in the way individuals perceive technological innovations such as RFID. Business graduate students who are exposed to technological trends and their applications seemed to be more liberal about the uses of RFID. On the other hand, undergraduate students were more hesitant in accepting such applications, but they agreed on the uses of RFID that can help prevent theft and fraud.

Conclusions

The present study aimed at finding relationships between demographic backgrounds and their perceptions of privacy issues. However, findings revealed that privacy is an issue for all consumers. Graeff and Harmon (2002) found

that gender and income played a role in the way consumers perceive privacy (p. 310). Additionally, Monshi and Zieglmayer, (2004), found that ethnicity played a role in the way people perceive health issues and privacy.

The present study focused on informational privacy and customers' attitudes towards it. Due to the unequal amount of respondents representing each demographic group (gender, age, ethnicity, education) the results of the study did not reveal significant differences between them. However, there was a difference between graduate and undergraduate students and their knowledge of RFID technologies. The majority of the students that indicated that had heard of RFID were graduate students. However, since the majority of the students were undergraduates and only a small percentage of them indicated that they have heard of RFID in the past, the responses towards possible uses of RFID were mostly indifferent. However, they were less hesitant in accepting RFID uses to prevent theft, counterfeit medications, and to find stolen items.

In addition, the fact that the graduate students were from the school of Business increased the likelihood of having a broader knowledge of technological innovations and their implementations. They indicated that it was acceptable to use RFID to collect customers' information,

to receive discounts, and to monitor patients' compliance with medications.

The selection of specific classes (2 business classes and 1 psychology class) and the small scale of the sample constrained the results of the study. However, it is important to note that the educational background of the respondents aided in understanding new technologies and its usages.

Implications and Future Research

The limitations and the use of a convenience sample did not allow generalizing the results. However, given that the topic of this research is fairly new and has not gained much interest there is still an opportunity for further study. An important note to have in mind when conducting future research on this topic is to expand the scope of the population and sample. It is very likely that if data was collected from different countries, knowing that the participants who represent each ethnic group were influenced by their cultures, then there may be significant findings. As anticipated in the present study, education seemed to have an influence in the manner people perceived privacy issues. Educational background and privacy perceptions should be studied further.

Future research in this area is important for several reasons. Privacy concerns are on the rise; however, not just privacy, but the violation of identity theft. It will be very helpful if researchers can identify why and what factors contribute to growing concerns about informational privacy. The more that information exists regarding this more it will help in developing laws that will protect individuals' privacy.

Organizations need to have a better understanding of their customers' attitudes towards privacy. This understanding will provide organizations with information on how to create trustful and long-term relationships between them and their customers. In addition, as a part of their CRM strategies and personalized relationships, organizations will have the chance to treat each customer's privacy based on the customers' specifications. If these requirements are met then trusting relationships can be established, and the benefits of CRM can be enjoyed by both the company and the customer.

Having knowledge about how people from different cultures perceive informational privacy will be vital in global marketing efforts to build lifetime customers. This notion is also supported by Singh and Hill (2003): "understanding how consumers in a country view privacy

issues provides a means to understanding whether people will be open to marketing efforts which require information sharing and information exchange" (p. 647).

The results of this study along with previous research indicate that consumers view privacy policies to be very lengthy. Organizations need to establish simpler privacy policies that will encourage the consumers to read them.

In addition, organizations need to use encryptions when collecting information and they should be informing this on a continual basis.

RFID is recommended for retailers and manufacturers of higher end goods since those with higher education levels are more comfortable with it than those with a bachelors or lower degree.

APPENDIX A

SURVEY

INFORMED CONSENT

The survey in which you are being asked to participate has a purpose to study consumers' attitudes towards privacy issues. This study is being conducted by Maria Nicolaou under the supervision of Dr. Nabil Razzouk and Dr. Victoria Seitz, professors of the Marketing Department. This research has been reviewed and approved by the Institutional Review Board, California State University, San Bernardino.

In this survey you will be asked to indicate your responses to several statements by using the given rating scales. The survey should take about 15 to 20 minutes to complete. The information you will provide in this survey will be anonymous, and will be used only for the purposes of this study. If you wish to receive the results of this study, the complete research will be available at the Pfau Library, at CSUSB in January 2007.

Your participation in this study is totally voluntary. You have the option to refuse participation and without penalty. Upon completion of this survey and at your instructor's discretion, you may receive a slip for one unit of extra credit. In order to ensure the validity of the study, we ask that you not discuss this study with other students or participants. If you do not wish to participate in this survey you may proceed to the assigned reading of your class.

There are no foreseeable risks related to this study. Since the topic being studied is fairly new to research, the results of this study may add valuable information to this emerging research field.

If you have any questions or concerns about this study, please feel free to contact me, Dr. Nabil Razzouk, at (909) 537- 5754.

By placing a check mark in the space provided below, I acknowledge that I have been informed of, and that I understand, the nature and purpose of this study, and I freely consent to participate. I also acknowledge that I am at least 18 years of age.

Place a check mark here: _____ **Today's date:** _____

Consumer Opinion Survey

The purpose of this survey is to assess consumer attitudes towards individual privacy issues. The research is a part of the requirement for the completion of my Masters Program. Your assistance would be greatly appreciated. Please complete all the questions. Your responses will be anonymous.

Thank You _____

1) When conducting business with organizations, how important to you is each of the following? Please use the 1-5 scale by circling one number for each statement.	Very Unimportant	Somewhat Unimportant	**Indifferent**	Somewhat Important	Very Important
a) Protecting the privacy of my information	1	2	3	4	5
b) Good Customer Service	1	2	3	4	5
c) Product/Service Satisfaction	1	2	3	4	5
d) Cost of product/service	1	2	3	4	5
e) Personalized relationship	1	2	3	4	5
f) Mutual Trust	1	2	3	4	5
g) Knowledgeable staff	1	2	3	4	5
h) Accessibility i.e. web site, call centers	1	2	3	4	5
i) Availability; extensive customer service hours	1	2	3	4	5
j) The option to opt in or opt out when asked to disclose personal information	1	2	3	4	5
k) Selection of merchandise/services	1	2	3	4	5
l) Feedback on my requests, complaints, suggestions	1	2	3	4	5
m) Convenient shopping	1	2	3	4	5
n) Frequent Buyer Reward Program	1	2	3	4	5
o) Fast problem resolution	1	2	3	4	5
p) Compensation/rewards for inconvenience	1	2	3	4	5
q) Tailored services based on my needs and demands	1	2	3	4	5
r) Human-to-Human interaction	1	2	3	4	5

Next Page please

2) Using the following scale, how would you rate the "privacy" level of each of the following information items? Circle one number for each statement Personal Information items:	Definitely Private and always protected; I would not share with businesses 1	Somewhat Private, share with family and friends, and used in normal transactions 2	Indifferent 3	Private, but willing to share occasionally and on a limited basis only 4	Private, but less hesitant to share with organizations I conduct business with. 5
a) Social Security Number	1	2	3	4	5
b) Mailing Address	1	2	3	4	5
c) E-mail Address	1	2	3	4	5
d) Credit Card Number	1	2	3	4	5
e) Home Telephone Number	1	2	3	4	5
f) Occupation	1	2	3	4	5
g) Annual Income	1	2	3	4	5
h) Ethnicity	1	2	3	4	5
i) Employer	1	2	3	4	5
j) Owned assets	1	2	3	4	5
k) Owned investments	1	2	3	4	5
l) Place of birth	1	2	3	4	5
m) Date of birth	1	2	3	4	5
n) Legal history	1	2	3	4	5
o) Mother's maiden name	1	2	3	4	5
p) Health related information	1	2	3	4	5
q) Places lived	1	2	3	4	5
r) Number of children	1	2	3	4	5
s) Sexual Orientation	1	2	3	4	5
t) Home expenses	1	2	3	4	5
u) Work Phone Number	1	2	3	4	5
v) Wireless Telephone Number	1	2	3	4	5
w) Gender	1	2	3	4	5
x) Citizenship	1	2	3	4	5
y) Passport Number	1	2	3	4	5
z) Driver's License/ ID number	1	2	3	4	5

Next Page please

	Scenario #1	Scenario #2	Scenario #3	Scenario #4
3) a)Which of the scenarios have you experienced in the last 12 months? Place an X in the appropriate cell.	Buying a car from a dealership	Buying Auto Insurance	Making on-line reservations for a hotel	Making a credit card purchase of electronics
3) b) For each of the scenarios which personal information items are you willing to disclose? Please place the number "1" in the cell by each item you are willing to disclose information for each of the scenarios				
a) Social Security Number				
b) Employer				
c) E-mail Address				
d) Credit Card Number				
e) Telephone Number				
f) Occupation				
g) Annual Income				
h) Ethnicity				
i) Mailing Address				
j) Owned assets				
k) Owned investments				
l) Place of birth				
m) Date of birth				
n) Legal history				
o) Mother's maiden name				
p) Health related information				
q) Gender				
r) Number of children				
s) Sexual Orientation				
t) Home expenses				
u) Work Telephone Number				
v) Wireless Telephone Number				
w) Driver's License/ ID Number				
x) Citizenship				
y) Passport Number				
z) Places Lived				

Next Page please

4) For each of the statements below indicate your level of agreement or disagreement by circling a number from 1 to 5.	Strongly Disagree 1	Disagree 2	Undecided 3	Agree 4	Strongly Agree 5
a) I am aware of the risks when I disclose my personal information	1	2	3	4	5
b) I feel that I lost control over my privacy	1	2	3	4	5
c) I am constantly worrying about my finances	1	2	3	4	5
d) I always look for the privacy policy before I disclose personal information to a company	1	2	3	4	5
e) I disclose my personal information only to companies I trust.	1	2	3	4	5
f) I feel that I am monitored by companies that have my personal information	1	2	3	4	5
g) As a consumer I am aware of all the legal protections that I have for my private information	1	2	3	4	5
h) I always make sure that my personal information will not be shared with third parties	1	2	3	4	5
i) I read carefully the privacy notices I receive from companies I do businesses with.	1	2	3	4	5
j) I am always afraid to give information on the internet	1	2	3	4	5
k) I am always afraid to give information over the phone	1	2	3	4	5
l) I consider invasion of privacy to be the use of my personal information without my consent	1	2	3	4	5
m) My privacy concerns influence my purchase behaviors	1	2	3	4	5
n) I feel unsafe with today's environment to disclose my private information	1	2	3	4	5

5) Have you ever heard of RFID (Radio Frequency Identifiers)? _____ YES _____NO

RFID are active microchips that will replace barcodes and will be implanted on products. Radio-frequency waves enable the tags to gather and transmit data regarding location, and/or identification.

The following questions pertain to the use of RFID in Business!

Next Page please

6) How would you rate the following uses of RFID in business? Circle one number for each statement	Very Acceptable 1	Somewhat Acceptable 2	Indifferent 3	Somewhat Unacceptable 4	Very unacceptable 5
a) As tags on merchandise in stores to prevent theft	1	2	3	4	5
b) As tags that are implanted in products to gather information after the purchase on product image, location and use, and transmit it to the vendors	1	2	3	4	5
c) As tags in the pharmaceutical industry that are implanted in drugs to prevent counterfeit medications	1	2	3	4	5
d) As tags on prescribed medications to identify the user and to insure appropriate compliance of the instructions by the patient.	1	2	3	4	5
e) As tags implanted on merchandise to insure safe transfer of products within supply chain (will insure that products are properly handled and not stolen)	1	2	3	4	5
f) As tags on store items that are deactivated at the point of sale, before a customer leaves the store.	1	2	3	4	5
g) As tags on purchased items that can transmit personal information of the customer to the vendors (i.e. age, address etc) for marketing purposes	1	2	3	4	5
h) As tags on prescribed medications to insure that they are dispersed properly and accurately by the pharmacist.	1	2	3	4	5
i) As tags on products that will provide discounts and special offers to customers who choose not to deactivate them at the point of sale.	1	2	3	4	5
j) As tags implanted in products that can help return stolen or lost products to their owners	1	2	3	4	5
k) RFID tags can be implanted in humans to increase access control to computer systems, medical records, buildings etc	1	2	3	4	5

Next Page please

For each of the questions below, circle the letter designate that best describes your response to questions 7-12. Your information will remain confidential.

7) Gender
(a) Male
(b) Female

8) Age group
(a) 18-24
(b) 25-36
(c) 37-48
(d) 49- 64
(e) 65 or older

9) Highest level of your education
(a) Some High School
(b) High School Graduate
(c) Some College
(d) Graduated College
(e) Post Graduate
(f) None of the above

10) Total household income in 2005.
(a) 0 - 20,999
(b) 21,000 - 40,999
(c) 41,000 - 50,999
(d) 51,000 – 60,999
(e) 61,000 or above

11) Current marital status
(a) Single, never married
(b) Married
(c) Separated
(d) Divorced
(e) Widowed

12) Race/ethnicity:
(a) White
(b) Black
(c) American Indian
(d) Asian / Middle Eastern
(e) Hispanic
(f) Other (please indicate): _____

APPENDIX B

FREQUENCY TABLES

Frequency Tables for Scenario 1- buying a car from a dealership

Social Security Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	41	20.2	27.9	27.9
	Yes	106	52.2	72.1	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Employer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	28	13.8	19.0	19.0
	Yes	119	58.6	81.0	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

E-mail Address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	74	36.5	50.3	50.3
	Yes	73	36.0	49.7	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Credit Card Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	84	41.4	57.1	57.1
	Yes	63	31.0	42.9	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Home Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	28	13.8	19.0	19.0
	Yes	119	58.6	81.0	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	31	15.3	21.1	21.1
	Yes	116	57.1	78.9	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Annual Income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	36	17.7	24.5	24.5
	Yes	111	54.7	75.5	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Ethnicity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	86	42.4	58.5	58.5
	Yes	61	30.0	41.5	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Mailing address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	25	12.3	17.0	17.0
	Yes	122	60.1	83.0	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Owned Assets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	108	53.2	73.5	73.5
	Yes	39	19.2	26.5	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Owned Investments

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	115	56.7	78.2	78.2
	Yes	32	15.8	21.8	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Place of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	96	47.3	65.3	65.3
	Yes	51	25.1	34.7	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Date of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	47	23.2	32.0	32.0
	Yes	100	49.3	68.0	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Legal History

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	117	57.6	79.6	79.6
	Yes	30	14.8	20.4	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Mother's maiden name

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	105	51.7	71.4	71.4
	Yes	42	20.7	28.6	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Health related information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	133	65.5	90.5	90.5
	Yes	14	6.9	9.5	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	63	31.0	42.9	42.9
	Yes	84	41.4	57.1	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Number of children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	119	58.6	81.0	81.0
	Yes	28	13.8	19.0	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Sexual Orientation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	118	58.1	80.3	80.3
	Yes	29	14.3	19.7	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Home expenses

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	105	51.7	71.4	71.4
	Yes	42	20.7	28.6	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Work Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	58	28.6	39.5	39.5
	Yes	89	43.8	60.5	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Wireless Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	65	32.0	44.2	44.2
	Yes	82	40.4	55.8	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Driver's License

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	34	16.7	23.1	23.1
	Yes	113	55.7	76.9	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Citizenship

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	90	44.3	61.2	61.2
	Yes	57	28.1	38.8	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Passport Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	138	68.0	93.9	93.9
	Yes	9	4.4	6.1	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Places lived

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	107	52.7	72.8	72.8
	Yes	40	19.7	27.2	100.0
	Total	147	72.4	100.0	
Missing	9	56	27.6		
Total		203	100.0		

Frequency Tables for Scenario 2 – buying auto insurance

Social Security Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	65	32.0	48.1	48.1
	Yes	70	34.5	51.9	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Employer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	57	28.1	42.2	42.2
	Yes	78	38.4	57.8	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

E-mail Address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	68	33.5	50.4	50.4
	Yes	67	33.0	49.6	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Credit Card Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	91	44.8	67.4	67.4
	Yes	44	21.7	32.6	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Home Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	21	10.3	15.6	15.6
	Yes	114	56.2	84.4	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	44	21.7	32.6	32.6
	Yes	91	44.8	67.4	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Annual Income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	82	40.4	60.7	60.7
	Yes	53	26.1	39.3	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Ethnicity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	78	38.4	57.8	57.8
	Yes	57	28.1	42.2	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Mailing address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	19	9.4	14.1	14.1
	Yes	115	56.7	85.2	99.3
	2	1	.5	.7	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Owned Assets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	116	57.1	85.9	85.9
	Yes	19	9.4	14.1	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Owned Investments

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	125	61.6	92.6	92.6
	Yes	10	4.9	7.4	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Place of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	95	46.8	70.4	70.4
	Yes	40	19.7	29.6	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Date of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	43	21.2	31.9	31.9
	Yes	92	45.3	68.1	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Legal History

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	106	52.2	78.5	78.5
	Yes	29	14.3	21.5	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Mother's maiden name

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	108	53.2	80.0	80.0
	Yes	27	13.3	20.0	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Health related information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	104	51.2	77.0	77.0
	Yes	31	15.3	23.0	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	49	24.1	36.3	36.3
	Yes	86	42.4	63.7	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Number of children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	93	45.8	68.9	68.9
	Yes	42	20.7	31.1	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Sexual Orientation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	112	55.2	83.0	83.0
	Yes	23	11.3	17.0	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Home expenses

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	116	57.1	85.9	85.9
	Yes	19	9.4	14.1	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Work Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	66	32.5	48.9	48.9
	Yes	69	34.0	51.1	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Wireless Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	61	30.0	45.2	45.2
	Yes	74	36.5	54.8	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Driver's License

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	26	12.8	19.3	19.3
	Yes	109	53.7	80.7	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Citizenship

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	83	40.9	61.5	61.5
	Yes	52	25.6	38.5	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Passport Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	127	62.6	94.1	94.1
	Yes	8	3.9	5.9	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Places lived

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	114	56.2	84.4	84.4
	Yes	21	10.3	15.6	100.0
	Total	135	66.5	100.0	
Missing	9	68	33.5		
Total		203	100.0		

Frequency Tables for Scenario 3 – making on-line reservations for a hotel

Social Security Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	137	67.5	95.1	95.1
	Yes	7	3.4	4.9	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Employer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	132	65.0	91.7	91.7
	Yes	12	5.9	8.3	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

E-mail Address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	30	14.8	20.8	20.8
	Yes	114	56.2	79.2	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Credit Card Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	25	12.3	17.5	17.5
	Yes	118	58.1	82.5	100.0
	Total	143	70.4	100.0	
Missing	9	59	29.1		
	System	1	.5		
	Total	60	29.6		
Total		203	100.0		

Home Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	36	17.7	25.0	25.0
	Yes	108	53.2	75.0	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	116	57.1	80.6	80.6
	Yes	28	13.8	19.4	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Annual Income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	135	66.5	93.8	93.8
	Yes	9	4.4	6.3	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Ethnicity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	102	50.2	70.8	70.8
	Yes	42	20.7	29.2	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Mailing address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	37	18.2	25.7	25.7
	Yes	107	52.7	74.3	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Owned Assets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	141	69.5	97.9	97.9
	Yes	3	1.5	2.1	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Owned Investments

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	141	69.5	97.9	97.9
	Yes	3	1.5	2.1	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Place of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	121	59.6	84.0	84.0
	Yes	23	11.3	16.0	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Date of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	89	43.8	61.8	61.8
	Yes	55	27.1	38.2	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Legal History

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	131	64.5	91.0	91.0
	Yes	13	6.4	9.0	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Mother's maiden name

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	130	64.0	90.3	90.3
	Yes	14	6.9	9.7	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Health related information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	135	66.5	93.8	93.8
	Yes	9	4.4	6.3	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	95	46.8	66.0	66.0
	Yes	49	24.1	34.0	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Number of children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	113	55.7	78.5	78.5
	Yes	31	15.3	21.5	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Sexual Orientation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	118	58.1	81.9	81.9
	Yes	26	12.8	18.1	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Home expenses

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	137	67.5	95.1	95.1
	Yes	7	3.4	4.9	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Work Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	107	52.7	74.3	74.3
	Yes	37	18.2	25.7	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Wireless Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	80	39.4	55.6	55.6
	Yes	64	31.5	44.4	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Driver's License

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	121	59.6	84.0	84.0
	Yes	23	11.3	16.0	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Citizenship

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	114	56.2	79.2	79.2
	Yes	30	14.8	20.8	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Passport Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	138	68.0	95.8	95.8
	Yes	6	3.0	4.2	100.0
	Total	144	70.9	100.0	
Missing	9	59	29.1		
Total		203	100.0		

Places lived

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	130	64.0	89.7	89.7
	Yes	15	7.4	10.3	100.0
	Total	145	71.4	100.0	
Missing	9	58	28.6		
Total		203	100.0		

Frequency Tables for Scenario 4 – making credit card purchases of electronics

Social Security Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	139	68.5	93.3	93.3
	Yes	10	4.9	6.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Employer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	130	64.0	87.2	87.2
	Yes	19	9.4	12.8	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

E-mail Address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	55	27.1	36.9	36.9
	Yes	94	46.3	63.1	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Credit Card Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	25	12.3	16.8	16.8
	Yes	123	60.6	82.6	99.3
	2	1	.5	.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Home Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	57	28.1	38.3	38.3
	Yes	92	45.3	61.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	124	61.1	83.2	83.2
	Yes	25	12.3	16.8	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Annual Income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	140	69.0	94.0	94.0
	Yes	9	4.4	6.0	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Ethnicity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	112	55.2	75.2	75.2
	Yes	37	18.2	24.8	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Mailing address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	42	20.7	28.2	28.2
	Yes	107	52.7	71.8	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Owned Assets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	148	72.9	99.3	99.3
	Yes	1	.5	.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Owned Investments

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	148	72.9	99.3	99.3
	Yes	1	.5	.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Place of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	131	64.5	87.9	87.9
	Yes	18	8.9	12.1	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Date of birth

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	105	51.7	70.5	70.5
	Yes	44	21.7	29.5	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Legal History

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	141	69.5	94.6	94.6
	Yes	8	3.9	5.4	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Mother's maiden name

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	136	67.0	91.3	91.3
	Yes	13	6.4	8.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Health related information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	141	69.5	94.6	94.6
	Yes	8	3.9	5.4	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	109	53.7	73.2	73.2
	Yes	40	19.7	26.8	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Number of children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	135	66.5	90.6	90.6
	Yes	14	6.9	9.4	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Sexual Orientation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	127	62.6	85.2	85.2
	Yes	22	10.8	14.8	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Home expenses

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	145	71.4	97.3	97.3
	Yes	4	2.0	2.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Work Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	120	59.1	80.5	80.5
	Yes	29	14.3	19.5	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Wireless Telephone Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	106	52.2	71.1	71.1
	Yes	43	21.2	28.9	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Driver's License

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	123	60.6	82.6	82.6
	Yes	26	12.8	17.4	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Citizenship

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	120	59.1	80.5	80.5
	Yes	29	14.3	19.5	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Passport Number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	145	71.4	97.3	97.3
	Yes	4	2.0	2.7	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Places lived

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	132	65.0	88.6	88.6
	Yes	13	6.4	8.7	97.3
	2	1	.5	.7	98.0
	4	3	1.5	2.0	100.0
	Total	149	73.4	100.0	
Missing	9	54	26.6		
Total		203	100.0		

Frequency Tables for RFID uses

As tags on merchandise in stores to prevent theft

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	104	51.2	53.3	53.3
	Somewhat Acceptable	52	25.6	26.7	80.0
	Indifferent	16	7.9	8.2	88.2
	Somewhat Unacceptable	10	4.9	5.1	93.3
	Very unacceptable	13	6.4	6.7	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

As tags that are implanted in products to gather information after the purchase on product image, location and use, and transmit it to vendors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	18	8.9	9.2	9.2
	Somewhat Acceptable	27	13.3	13.8	23.1
	Indifferent	26	12.8	13.3	36.4
	Somewhat Unacceptable	47	23.2	24.1	60.5
	Very unacceptable	77	37.9	39.5	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

As tags in the pharmaceutical industry that are implanted in drugs to prevent counterfeit medications

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	50	24.6	25.6	25.6
	Somewhat Acceptable	68	33.5	34.9	60.5
	Indifferent	33	16.3	16.9	77.4
	Somewhat Unacceptable	19	9.4	9.7	87.2
	Very unacceptable	25	12.3	12.8	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

As tags on prescribed medications to identify the user and to insure appropriate compliance of the instructions by the patient

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	26	12.8	13.3	13.3
	Somewhat Acceptable	42	20.7	21.5	34.9
	Indifferent	32	15.8	16.4	51.3
	Somewhat Unacceptable	57	28.1	29.2	80.5
	Very unacceptable	38	18.7	19.5	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

As tags implanted on merchandise to insure safe transfer of products within supply chain (will insure that products are

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	59	29.1	30.4	30.4
	Somewhat Acceptable	76	37.4	39.2	69.6
	Indifferent	32	15.8	16.5	86.1
	Somewhat Unacceptable	16	7.9	8.2	94.3
	Very unacceptable	11	5.4	5.7	100.0
	Total	194	95.6	100.0	
Missing	9	9	4.4		
Total		203	100.0		

As tags on store items that are deactivated at the point of sale, before the customer leaves the store

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	97	47.8	49.7	49.7
	Somewhat Acceptable	55	27.1	28.2	77.9
	Indifferent	16	7.9	8.2	86.2
	Somewhat Unacceptable	14	6.9	7.2	93.3
	Very unacceptable	13	6.4	6.7	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

As tags on purchased items that can transmit personal information of the customer to the vendors (i.e. age, address, etc) for marketing purposes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	19	9.4	9.7	9.7
	Somewhat Acceptable	7	3.4	3.6	13.3
	Indifferent	20	9.9	10.3	23.6
	Somewhat Unacceptable	28	13.8	14.4	37.9
	Very unacceptable	121	59.6	62.1	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

As tags on prescribed medications to insure the they are dispersed properly and accurately by the pharmacist

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	44	21.7	22.8	22.8
	Somewhat Acceptable	62	30.5	32.1	54.9
	Indifferent	48	23.6	24.9	79.8
	Somewhat Unacceptable	22	10.8	11.4	91.2
	Very unacceptable	17	8.4	8.8	100.0
	Total	193	95.1	100.0	
Missing	9	10	4.9		
Total		203	100.0		

As tags on products that will provide discounts and special offers to customers who choose not to deactivate them at the point of sale

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	21	10.3	10.8	10.8
	Somewhat Acceptable	40	19.7	20.5	31.3
	Indifferent	57	28.1	29.2	60.5
	Somewhat Unacceptable	39	19.2	20.0	80.5
	Very unacceptable	38	18.7	19.5	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

RFID tags can be implanted in humans to increase access control to computer systems, medical records, building etc.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Acceptable	12	5.9	6.2	6.2
	Somewhat Acceptable	19	9.4	9.7	15.9
	Indifferent	29	14.3	14.9	30.8
	Somewhat Unacceptable	22	10.8	11.3	42.1
	Very unacceptable	113	55.7	57.9	100.0
	Total	195	96.1	100.0	
Missing	9	8	3.9		
Total		203	100.0		

APPENDIX C

CROSS TABULATIONS

Crosstabs: Question 1 and Data Collection

protecting the privacy of my information * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
protecting the privacy of my information	Very Unimportant	6		13	19
	Somewhat Unimportant			1	1
	Indifferent	1	1	2	4
	Somewhat Important	5	2	10	17
	Very Important	60	11	91	162
Total		72	14	117	203

Good customer service * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Good customer service	Very Unimportant	4		12	16
	Somewhat Unimportant	2		3	5
	Indifferent			6	6
	Somewhat Important	10	2	18	30
	Very Important	56	12	78	146
Total		72	14	117	203

Product/Service satisfaction * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Product/Service satisfaction	Very Unimportant	5		13	18
	Somewhat Unimportant	1		2	3
	Indifferent			6	6
	Somewhat Important	7	1	16	24
	Very Important	59	13	79	151
Total		72	14	116	202

Cost of product/service * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Cost of product/service	Very Unimportant	4		8	12
	Somewhat Unimportant	2		6	8
	Indifferent	6	1	9	16
	Somewhat Important	23	9	31	63
	Very Important	36	4	61	101
Total		71	14	115	200

Personalized relationship * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Personalized relationship	Very Unimportant	2		8	10
	Somewhat Unimportant	7	1	19	27
	Indifferent	26	2	42	70
	Somewhat Important	23	11	29	63
	Very Important	13		19	32
Total		71	14	117	202

Mutual Trust * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Mutual Trust	Very Unimportant	4		10	14
	Somewhat Unimportant	1		5	6
	Indifferent	3	1	16	20
	Somewhat Important	31	7	32	70
	Very Important	32	5	52	89
Total		71	13	115	199

Knowledgeable Staff * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Knowledgeable Staff	Very Unimportant	4		10	14
	Somewhat Unimportant	1		6	7
	Indifferent	3		11	14
	Somewhat Important	23	8	19	50
	Very Important	40	6	71	117
Total		71	14	117	202

Accessibility i.e. web site, call centers * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Accessibility i.e. web site, call centers	Very Unimportant	5		9	14
	Somewhat Unimportant	2		9	11
	Indifferent	9	2	14	25
	Somewhat Important	29	8	37	74
	Very Important	27	4	48	79
Total		72	14	117	203

Availability; extensive customer service hours * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Availability; extensive customer service hours	Very Unimportant	5		9	14
	Somewhat Unimportant	2		7	9
	Indifferent	7	6	18	31
	Somewhat Important	33	6	39	78
	Very Important	25	2	44	71
Total		72	14	117	203

The option to opt in or opt out when asked to disclose personal information * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
The option to opt in or opt out when asked to disclose personal information	Very Unimportant	6		12	18
	Somewhat Unimportant	3		5	8
	Indifferent	10	3	13	26
	Somewhat Important	17	8	29	54
	Very Important	35	3	58	96
Total		71	14	117	202

Selection of merchantise/services * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Selection of merchantise/services	Very Unimportant	4		7	11
	Somewhat Unimportant	2		11	13
	Indifferent	3		9	12
	Somewhat Important	32	12	39	83
	Very Important	31	2	49	82
Total		72	14	115	201

Feedback on my requests, complaints, suggestions * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Feedback on my requests, complaints, suggestions	Very Unimportant	2		9	11
	Somewhat Unimportant	8		13	21
	Indifferent	13	3	18	34
	Somewhat Important	18	6	43	67
	Very Important	31	5	34	70
Total		72	14	117	203

convenient shopping * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
convenient shopping	Very Unimportant	4		5	9
	Somewhat Unimportant	4		14	18
	Indifferent	4	2	13	19
	Somewhat Important	27	7	36	70
	Very Important	33	5	49	87
Total		72	14	117	203

Frequent Buyer Reward Program * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Frequent Buyer Reward Program	Very Unimportant	4		8	12
	Somewhat Unimportant	12	3	17	32
	Indifferent	21	6	39	66
	Somewhat Important	20	4	26	50
	Very Important	15	1	26	42
Total		72	14	116	202

Fast problem resolution * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Fast problem resolution	Very Unimportant	6		9	15
	Somewhat Unimportant	1		11	12
	Indifferent	4	2	10	16
	Somewhat Important	20	5	23	48
	Very Important	41	7	64	112
Total		72	14	117	203

Compansation/rewards for inconvenience * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Compansation/rewards for inconvenience	Very Unimportant	6		8	14
	Somewhat Unimportat	2	2	11	15
	Indifferent	10	3	16	29
	Somewhat Important	28	6	42	76
	Very Important	26	3	38	67
Total		72	14	115	201

Tailored services based on my needs and demands * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Tailored services based on my needs and demands	Very Unimportant	4		5	9
	Somewhat Unimportant	3		15	18
	Indifferent	10	6	25	41
	Somewhat Important	36	6	40	82
	Very Important	19	2	31	52
Total		72	14	116	202

Human-to-human interaction * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Human-to-human interaction	Very Unimportant	3		9	12
	Somewhat Unimportant	4	2	16	22
	Indifferent	11	3	19	33
	Somewhat Important	26	7	29	62
	Very Important	28	2	44	74
Total		72	14	117	203

Crosstabs: Question 2 and Data Collection

Social Security Number * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Social Security Number	Definetely Private and always protected; I would not share w	39	11	82	132
	Somewhat Private;share with family and friends and used in n	12	1	17	30
	Indifferent		1		1
	Private but willing to share occassionally and on a limited	12		10	22
	Private but less hesitant to share with organizations I cond	9	1	7	17
Total		72	14	116	202

Mailing Address * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Mailing Address	Definetely Private and always protected; I would not share w	4	4	9	17
	Somewhat Private;share with family and friends and used in n	30	1	55	86
	Indifferent	15	2	14	31
	Private but willing to share occassionally and on a limited	13	6	26	45
	Private but less hesitant to share with organizations I cond	10	1	12	23
Total		72	14	116	202

E-mail Address * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
E-mail Address	Definetely Private and always protected; I would not share w	1	1	7	9
	Somewhat Private;share with family and friends and used in n	32	3	43	78
	Indifferent	16	3	24	43
	Private but willing to share occassionally and on a limited	11	3	22	36
	Private but less hesitant to share with organizations I cond	12	4	19	35
Total		72	14	115	201

Credit Card Number * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Credit Card Number	Definetely Private and always protected; I would not share w	36	8	57	101
	Somewhat Private;share with family and friends and used in n	12	3	35	50
	Indifferent			4	4
	Private but willing to share occassionally and on a limited	10	2	11	23
	Private but less hesitant to share with organizations I cond	14	1	9	24
Total		72	14	116	202

Home Telephone Number * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Home Telephone Number	Definetely Private and always protected; I would not share w	10	4	21	35
	Somewhat Private;share with family and friends and used in n	24	1	49	74
	Indifferent	17	1	16	34
	Private but willing to share occassionally and on a limited	16	5	19	40
	Private but less hesitant to share with organizations I cond	5	3	11	19
Total		72	14	116	202

Occupation * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Occupation	Definetely Private and always protected; I would not share w		2	7	9
	Somewhat Private;share with family and friends and used in n	14	2	28	44
	Indifferent	30	5	44	79
	Private but willing to share occassionally and on a limited	15	1	15	31
	Private but less hesitant to share with organizations I cond	13	4	22	39
Total		72	14	116	202

Annual Income * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Annual Income	Definetely Private and always protected; I would not share w	15	5	24	44
	Somewhat Private;share with family and friends and used in n	17	3	30	50
	Indifferent	20	4	27	51
	Private but willing to share occassionally and on a limited	13	2	19	34
	Private but less hesitant to share with organizations I cond	6		15	21
Total		71	14	115	200

Ethnicity * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Ethnicity	Definetely Private and always protected; I would not share w	3	2	9	14
	Somewhat Private;share with family and friends and used in n	6	2	13	21
	Indifferent	36	6	55	97
	Private but willing to share occassionally and on a limited	12	2	12	26
	Private but less hesitant to share with organizations I cond	14	2	27	43
Total		71	14	116	201

Employer * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Employer	Definetely Private and always protected; I would not share w	3	2	5	10
	Somewhat Private;share with family and friends and used in n	13	2	23	38
	Indifferent	32	4	49	85
	Private but willing to share occassionally and on a limited	9	4	16	29
	Private but less hesitant to share with organizations I cond	15	2	23	40
Total		72	14	116	202

Owned Assets * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Owned Assets	Definetely Private and always protected; I would not share w	20	7	46	73
	Somewhat Private;share with family and friends and used in n	26	3	28	57
	Indifferent	13	2	22	37
	Private but willing to share occassionally and on a limited	6	2	7	15
	Private but less hesitant to share with organizations I cond	7		12	19
Total		72	14	115	201

Owned Investments * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Owned Investments	Definetely Private and always protected; I would not share w	27	7	53	87
	Somewhat Private;share with family and friends and used in n	17	3	19	39
	Indifferent	14	2	22	38
	Private but willing to share occassionally and on a limited	7	2	7	16
	Private but less hesitant to share with organizations I cond	6		14	20
Total		71	14	115	200

Place of birth * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Place of birth	Definetely Private and always protected; I would not share w	5	2	13	20
	Somewhat Private;share with family and friends and used in n	14	2	23	39
	Indifferent	33	4	45	82
	Private but willing to share occassionally and on a limited	8	4	14	26
	Private but less hesitant to share with organizations I cond	12	2	21	35
Total		72	14	116	202

Date of birth * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Date of birth	Definetely Private and always protected; I would not share w	3	2	14	19
	Somewhat Private;share with family and friends and used in n	16	2	27	45
	Indifferent	33	5	41	79
	Private but willing to share occassionally and on a limited	7	4	16	27
	Private but less hesitant to share with organizations I cond	13	1	18	32
Total		72	14	116	202

Legal History * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Legal History	Definetely Private and always protected; I would not share w	20	5	61	86
	Somewhat Private;share with family and friends and used in n	12	2	13	27
	Indifferent	24	5	28	57
	Private but willing to share occassionally and on a limited	11	1	7	19
	Private but less hesitant to share with organizations I cond	5	1	7	13
Total		72	14	116	202

Mother's maiden name * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Mother's maiden name	Definetely Private and always protected; I would not share w	16	6	42	64
	Somewhat Private;share with family and friends and used in n	27	1	27	55
	Indifferent	18	4	24	46
	Private but willing to share occassionally and on a limited	6	3	9	18
	Private but less hesitant to share with organizations I cond	5		14	19
Total		72	14	116	202

Health related information * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Health related information	Definetely Private and always protected; I would not share w	18	7	51	76
	Somewhat Private;share with family and friends and used in n	23	1	33	57
	Indifferent	20	3	17	40
	Private but willing to share occassionally and on a limited	7	2	8	17
	Private but less hesitant to share with organizations I cond	4	1	7	12
Total		72	14	116	202

Places lived * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Places lived	Definetely Private and always protected; I would not share w	6	4	13	23
	Somewhat Private;share with family and friends and used in n	14	3	33	50
	Indifferent	34	2	43	79
	Private but willing to share occassionally and on a limited	12	4	11	27
	Private but less hesitant to share with organizations I cond	6	1	15	22
Total		72	14	115	201

Number of children * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Number of children	Definetely Private and always protected; I would not share w	7	1	10	18
	Somewhat Private;share with family and friends and used in n	9	3	19	31
	Indifferent	37	8	56	101
	Private but willing to share occassionally and on a limited	6	2	15	23
	Private but less hesitant to share with organizations I cond	13		16	29
Total		72	14	116	202

Sexual Orientation * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Sexual Orientation	Definetely Private and always protected; I would not share w	10	2	19	31
	Somewhat Private;share with family and friends and used in n	6	1	15	22
	Indifferent	34	5	54	93
	Private but willing to share occassionally and on a limited	5	2	10	17
	Private but less hesitant to share with organizations I cond	16	4	17	37
Total		71	14	115	200

Home expenses * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Home expenses	Definetely Private and always protected; I would not share w	15	5	26	46
	Somewhat Private;share with family and friends and used in n	23	3	31	57
	Indifferent	17	4	37	58
	Private but willing to share occassionally and on a limited	7	2	15	24
	Private but less hesitant to share with organizations I cond	10		7	17
Total		72	14	116	202

Work Telephone Number * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Work Telephone Number	Definetely Private and always protected; I would not share w	10	1	25	36
	Somewhat Private;share with family and friends and used in n	26	4	40	70
	Indifferent	14	5	21	40
	Private but willing to share occassionally and on a limited	12	3	15	30
	Private but less hesitant to share with organizations I cond	10	1	15	26
Total		72	14	116	202

Wireless Telephone Number * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Wireless Telephone Number	Definetely Private and always protected; I would not share w	18	4	30	52
	Somewhat Private;share with family and friends and used in n	28	2	46	76
	Indifferent	6	6	9	21
	Private but willing to share occassionally and on a limited	12	2	17	31
	Private but less hesitant to share with organizations I cond	8		14	22
Total		72	14	116	202

Gender * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Gender	Definetely Private and always protected; I would not share w	5		6	11
	Somewhat Private;share with family and friends and used in n	6	3	14	23
	Indifferent	40	3	62	105
	Private but willing to share occassionally and on a limited	4	1	10	15
	Private but less hesitant to share with organizations I cond	17	7	24	48
Total		72	14	116	202

Citizenship * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Citizenship	Definetely Private and always protected; I would not share w	4	1	12	17
	Somewhat Private;share with family and friends and used in n	5	1	14	20
	Indifferent	38	5	54	97
	Private but willing to share occassionally and on a limited	7		11	18
	Private but less hesitant to share with organizations I cond	18	6	25	49
Total		72	13	116	201

Passport Number * Data Collection Crosstabulation

Count

		Data Collection			Total
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	
Passport Number	Definetely Private and always protected; I would not share w	38	9	74	121
	Somewhat Private;share with family and friends and used in n	12	3	15	30
	Indifferent	7		15	22
	Private but willing to share occassionally and on a limited	6	1	2	9
	Private but less hesitant to share with organizations I cond	9	1	10	20
Total		72	14	116	202

Driver's License/ID Number * Data Collection Crosstabulation

Count

		Data Collection			Total
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	
Driver's License/ID Number	Definetely Private and always protected; I would not share w	26	6	54	86
	Somewhat Private;share with family and friends and used in n	17	4	30	51
	Indifferent	4		8	12
	Private but willing to share occassionally and on a limited	16	3	10	29
	Private but less hesitant to share with organizations I cond	9	1	14	24
Total		72	14	116	202

Crosstabs: Question 4 and Data Collection

am aware of the risks when I disclose personal information * Data Collection Crosstabulatior

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I am aware of the risks when I disclose personal information	Strongly Disagree			9	9
	Disagree	2		16	18
	Undecided	7	1	8	16
	Agree	37	9	50	96
	Strongly Agree	24	4	31	59
Total		70	14	114	198

I feel that I lost control over my privacy * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I feel that I lost control over my privacy	Strongly Disagree	3	1	10	14
	Disagree	24	5	29	58
	Undecided	23	1	30	54
	Agree	13	4	29	46
	Strongly Agree	8	3	16	27
Total		71	14	114	199

I am constantly worrying about my finances * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I am constantly worrying about my finances	Strongly Disagree	4		7	11
	Disagree	17	6	26	49
	Undecided	13	2	20	35
	Agree	30	5	41	76
	Strongly Agree	7	1	20	28
Total		71	14	114	199

ays look for the privacy policy before I disclose personal information to a company * Data Collec Crosstabulation

Count

		Data Collection			
		Business Undergradu ate students	Business Graduate Students	Psychology Undergaduat e students	Total
I always look for the privacy policy before I disclose personal information to a company	Strongly Disagree	7		10	17
	Disagree	14	1	31	46
	Undecided	10	7	25	42
	Agree	26	2	31	59
	Strongly Agree	14	4	17	35
Total		71	14	114	199

I disclose personal information only to companies I trust * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergradu ate students	Business Graduate Students	Psychology Undergaduat e students	Total
I disclose personal information only to companies I trust	Strongly Disagree	1		4	5
	Disagree	9	1	12	22
	Undecided	10		20	30
	Agree	33	6	49	88
	Strongly Agree	17	7	29	53
Total		70	14	114	198

I feel that I am monitored by companies that have my personal information * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergradu ate students	Business Graduate Students	Psychology Undergaduat e students	Total
I feel that I am monitored by companies that have my personal information	Strongly Disagree	4	1	7	12
	Disagree	16	1	18	35
	Undecided	22	5	34	61
	Agree	23	2	35	60
	Strongly Agree	6	5	19	30
Total		71	14	113	198

s a consumer I am aware of all the legal protections that I have for my private information * Dat Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
As a consumer I am aware of all the legal protections that I have for my private information	Strongly Disagree	4		15	19
	Disagree	21	4	46	71
	Undecided	18	4	21	43
	Agree	20	4	22	46
	Strongly Agree	8	2	10	20
Total		71	14	114	199

I always make sure that my personal information will not be shared with third parties * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I always make sure that my personal information will not be shared with third parties	Strongly Disagree	5		10	15
	Disagree	12	4	32	48
	Undecided	10	1	19	30
	Agree	31	7	36	74
	Strongly Agree	13	2	17	32
Total		71	14	114	199

read carefully the privacy notices I receive from companies I do business with * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I read carefully the privacy notices I receive from companies I do business with	Strongly Disagree	10		14	24
	Disagree	15	5	38	58
	Undecided	12	4	13	29
	Agree	25	4	39	68
	Strongly Agree	9	1	10	20
Total		71	14	114	199

I am always afraid to give information on the internet * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I am always afraid to give information on the internet	Strongly Disagree	1	1	3	5
	Disagree	13	3	14	30
	Undecided	11	5	23	39
	Agree	26	5	38	69
	Strongly Agree	20		35	55
Total		71	14	113	198

I am always afraid to give information over the phone * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I am always afraid to give information over the phone	Strongly Disagree	1		2	3
	Disagree	15	3	13	31
	Undecided	6	4	19	29
	Agree	30	4	37	71
	Strongly Agree	19	3	43	65
Total		71	14	114	199

:onsider invasion of privacy to be the use of my personal information without my consent * Dat Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I consider invasion of privacy to be the use of my personal information without my consent	Strongly Disagree	1		3	4
	Disagree	4		2	6
	Undecided	4	4	6	14
	Agree	25	6	29	60
	Strongly Agree	37	4	74	115
Total		71	14	114	199

My privacy concerns influence my purchase behaviors * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
My privacy concerns influence my purchase behaviors	Strongly Disagree	4		6	10
	Disagree	5	1	14	20
	Undecided	21	3	36	60
	Agree	27	7	34	68
	Strongly Agree	14	3	24	41
Total		71	14	114	199

I feel unsafe with today's environment to disclose my personal information * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
I feel unsafe with today's environment to disclose my personal information	0	1	1		2
	Strongly Disagree	3		5	8
	Disagree	7	1	10	18
	Undecided	18	3	30	51
	Agree	21	7	37	65
	Strongly Agree	14	2	32	48
Total		64	14	114	192

Crosstabs: Question 5 and Data Collection

Have you ever heard of RFID? * Data Collection Crosstabulation

Count

		Data Collection			
		Business Undergraduate students	Business Graduate Students	Psychology Undergaduate students	Total
Have you ever heard of RFID?	No	57	9	104	170
	Yes	13	5	9	27
Total		70	14	113	197

REFERENCES

Ackerman, S. M., Cranor, L. F., & Reagle, J. (1999). Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *Electronic Commerce, 99, 1-8.* Retrieved from Emerald database August 20,2006.

Aldhizer, G. R., & Cashell, J. D. (2004). Customer Relationship Management: Risks and Control. *Internal Auditor,* 52. Retrieved February 4, 2004, from EBSCOhost (Academic Search Elite) database.

Berry, M. J. A., & Linoff, G.S. (2000). *Mastering Data Mining: The Art and Science of Customer Relationship Management.* New York: Wiley Computer Publishing.

Berson, A., Smith, S., & Thearling, K. (1999). *Building data mining applications for CRM.* New York: McGraw-Hill.

Cain, R. M. (2002). Global Privacy Concerns and Regulation- Is the United States a World Apart? *International Review of Law Computers and Technology, 16, 23.* Retrieved October 17, 2005 from Ebscohost Database.

Cannon, A. D. (2002). The Ethics of Database Marketing. *The Information Management Journal.* Retrieved March 16, 2005 from EBSCOhost (Academic Search Elite) Database.

Chye, K. H., & Gerry, C. K. L. (2002). Data Mining and Customer Relationship Marketing in the Banking Industry. *Singapore Management Review, 24,* 1. Retrieved October 24, 2004, from EBSCOhost (Academic Search Elite) database.

Clarkson, K. W., Miller, R. L., Jentz, G. A., & Cross, F. B. (2001). *West's Business Law* (8th ed.). Australia: West Legal Studies in Business.

Cohen, A. (2004). Nowhere to Hide. *PC magazine,* 129. Retrieved February 4, 2005, from EBSCOhost (Academic Search Elite) database.

Eckfeldt, B. (2005). What does RFID do for the Consumer?*Communications of the ACM, 48, 9, 77-79.* Retrieved June 10, 2006 from EBSCOhost database.

Evans, M. (2003). The Relational Oxymoron and Personalisation Pragmatism. *Journal of Consumer Marketing, 20,* 665. Retrieved July 17, 2005 from Emerald Database.

Fletcher, K. (2003). Consumer Power and Privacy: the changing nature of CRM. *International Journal of Advertising, 22,* 249-272. Retrieved January 30, 2005, from EBSCOhost (Academic Search Elite) database.

Gormley, K. (1992). One hundred Years of Privacy. *Wisconsin Law Review,* 1335. Retrieved January 22, 2005 from Lexis Nexis database.

Graeff, T. R. & Harmon S. (2002). Collecting and Using Personal Data: Consumers' awareness and concerns. *The Journal of Consumer Marketing, 19, 302-318.* Retrieved October 5, 2005, from Emerald Database.

Grossman, R. P. (1998). Developing and Managing effective consumer relationships. *Journal of Product & Brand Management,* 7, 27. Retrieved July 15, 2005 from Emerald Database.

Gunther, O. & Spiekermann, S. (2005). RFID and the Perception of Control: The Consumer's View. *Communication of the ACM, 48, 73-76.* Retrieved May 12, 2006 from EBSCOhost database.

Hubbell, A., & Redding, M. (2003). Customer Relationship Management - today and tomorrow. *The Journal of Bank Cost & Management, 16,* 44. Retrieved January 15, 2005, from ABI/Normal Database.

Jones, P., Clarke-Hill, C., Comfort, D., Hillier, D., & Shears, P. (2005). Radio Frequency Identification and food retailing in the UK. *British Food Journal, 107, 6, 356-361.* Retrieved June 2, 2005 from ABI/INFORM database.

Juban, R. L., & Wyld, D. C. (2004). Would you like chips with that?: Customer Perspectives of RFID. *Management Research News, 27, 11/12, 29-45.*

Kakalik, J. S., & Wright, M. A. (1996). Responding to privacy concerns of consumers. *Review of Business, 18,* 15. Retrieved October 24, 2004, from EBSCOhost (Academic Search Elite) database.

Kavali, S. G., Tzokas, N. X., & Saren, M. J.(1999). Relationship marketing as an ethical approach: philosophical and managerial considerations. *Management Decision, 37,* 573. Retrieved July 16, 2005 from Emerald Database.

Long, G., Hogg, M. K., Hartley, M., & Angold, S. J. (1999). Relationship Marketing and Privacy: exploring the thresholds. *Journal of Marketing Practice, 5,* 4. Retrieved July 15, 2005, from Emerald Database.

Monshi, B., & Zieglmayer, V. (2004). The Problem of Privacy in Transcultural Research: Reflections on an Ethnographic Study in Sri Lanka. *Ethics & Behavior*, 14, 4, 305-312. Retrieved March 20, 2006, from EBSCOhost Database.

Orwell, G. (1949). *1984.* New York: Harcourt, Brace and Company.

Pitta, D. A., Franzak, F., & Laric, M. (2003). Privacy and one- to-one marketing: resolving the conflict. *Journal of Consumer Marketing, 20,* 616. Retrieved February 4, 2005, from Emerald database.

Ronald B. Standler (1998, May). *Privacy law in the USA.* Retrieved October 24, 2004, from http://www.rbs2.com/privacy.htm

Singh, T. and Hill, M. E. (2003). Consumer Privacy and the Internet in Europe: a view from Germany. *Journal of Consumer Marketing, 20, 7, 634-651.* Retrieved October 13, 2006 from Emerald Database.

Twist, D. C. (2005). The impact of radio frequency identification on supply chain facilities. *Journal of Facilities Management, 3, 3, 226-239.* Retrieved May 26, 2006 from Emerald database.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review.* Retrieved August 5, 2004, from http://www.lawrence.edu/fast/boardmaw/Privacy_brand_w a rr2.html

White, T. B. (2004). Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. *Journal of Consumer Psychology, 14, 41-51.* Retrieved Friday October 13, 2006 from EBSCOhost Database.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal, 113, 6, 1- 45.* Retrieved March 2, 2005 from Factiva Database.

Winer, R. S. (2001). A Framework for Customer Relationship Management. *California Management Review, 43.* Retrieved July 17, 2005 from Business Source Premier Database.