2010

Internet economy: Should the federal government intervene

Sha'Kera Bumbray

Internet Economy: Should the Federal Government Intervene

by Sha’Kera Bumbray

Masters of Science
Science, Technology and Public Policy
Thesis Submitted in Fulfillment of the
Graduation Requirements for the

College of Liberal Arts/Public Policy Program at
ROCHESTER INSTITUTE OF TECHNOLOGY
Rochester, New York

June 2010

Submitted by:

Sha’Kera Bumbray	Signature	Date

Accepted by:

Franz Foltz/Public Policy Rochester Institute of Technology	Signature	Date
John Angelis/Business Management Rochester Institute of Technology	Signature	Date
Danielle Smith/Sociology Rochester Institute of Technology	Signature	Date
Franz Foltz Graduate Coordinator/Public Policy Rochester Institute of Technology	Signature	Date
James Winebrake Department Chair/Public Policy Rochester Institute of Technology	Signature	Date

Table of Contents

Abstract

Global citizens choose to engage in electronic business every second of the day. The Internet has allowed for businesses to remain constantly open. All over the world people are able to conduct business quickly and cost effectively. Although the use of the Internet has significant benefits, there are also a number of risks. Most importantly there is a risk of the breach of personal security. This paper will use a patchwork design that consists of a case study and survey techniques to collect data on the use of business technologies by faculty and students at Rochester Institute of Technology (RIT). Each group will be issued the same survey to show the varying levels of participation in electronic business. Post collection, I propose that the data will show that although the majority of the RIT community engages in electronic business regularly, they remain concerned as to whether their information is being secured. I argue that both groups of faculty and students would like to see more federal involvement in electronic business to protect the average citizens’ personal privacy rights.

Chapter I

Introduction

E-Commerce has become a big part of American culture. It allows Americans to be able to shop online, pay bills online, bank online and to perform many other activities online. No longer are Americans limited to just what they can buy within the United States; e-commerce has allowed consumers and businesses alike to have a more global experience. Customers can save money or satisfy a desire to purchase foreign goods, and companies can outsource labor. There are many benefits to customers and business that choose to engage in electronic commerce. Consumers choose to engage in online activities to increase convenience, increase selection, and in terms of electronic banking, there is the possibility of a higher interest rate in comparison to more traditional banking. Businesses benefit from electronic commerce as well. Businesses can reach more customers despite geographic location, and are able to market their products at a lower cost. Electronic commerce also enables businesses to store information and conduct transactions less expensively. There are numerous benefits to government, consumers and businesses that choose to engage in the Internet economy.

The U.S. economy is in recession, although the online community is not experiencing the same difficulties. According to Rob Atkinson, president of the Information Technology and Innovation Foundation, "e-commerce [is] growing four to five times faster than traditional retail". Atkinson believes that e-commerce will continue to grow, based on current growth patterns. According to Forrester Research,

“Internet Economy: Should the Federal Government Intervene?”

> “Online retail sales, not including travel, reached US$175 billion in 2007, an increase of 21 percent from 2006. Forrester expects online sales to exceed $200 billion this year and exceed $300 billion in 2001.”(Gross, 2008)

This indicates that e-commerce is a growing industry and the growth should continue for the benefit of the U.S. economy. Although there are significant benefits to conducting business online, there are also a number of risks. The burdens of these risks are unevenly distributed, making the cost to the consumer much higher. Consumers are forced to trust websites with information, and risk their personal privacy and security. To minimize the risks faced by consumers, the government should be involved in the regulation of electronic commerce. The government has the power to restrict the harmful actions of companies, and ability to protect consumer information.

This research shows the experiences of a sample of the RIT community with electronic business. The RIT community for the purpose of this research will be defined as College of Liberal Arts faculty, and students enrolled in Liberal Arts classes. The thesis will display the high usage of electronic commerce by these groups. It will also show the commonality of security breaches within these groups. There is growing concern for the security of personal information among citizens. I argue that the research will support the thesis that average citizens find Internet security to be an important issue for which they would like to see greater government involvement.

At current, there is not a government mandate for a minimum level of security for companies that choose to engage in electronic business, which puts the information of anyone who interacts with this company at risk. The company is not inclined to have extra security protocols, as that will increase costs. Also, there is not a standard best practice for Internet security. As such, companies all have varying levels of security on their sites. Not only are these companies not federally required to have a minimum level of security, but these companies also have the right to collect consumer information and use it as they please. The consumer has no control over what information is gathered and who has access to it if they decide to engage in electronic business. For the purposes of this paper, there will be a public policy focus, as I attempt to show the failure of companies. As opposed to a science and technology issue, which would focus on the technology. An objective of the research is to show the necessity of federal intervention into the security protocols of electronic commerce.

Chapter 2

Literature Review

Definition of E-Commerce

Consumers now have access to the “24 hour economy,” according to Prins (2002). He defines Electronic commerce as, “all kinds of commercial dealings in the electronic world. Electronic commerce encompasses transactions of information, data, products, and services using online communication”. Prins makes it clear that electronic commerce and electronic business are two separate entities. Electronic business is used to describe the processes that a company conducts using a computer network. Examples of E-business include supply chain management systems or something as simple as exchanging documents enterprise wide; ability for multiple departments to access the same file. E-business can be used to describe any interaction both internally and externally that are translated through a computer, as opposed to electronic commerce, which is specially used to explain how companies interact with their clients and customers. E-commerce is, however a part of E-business, although E-business does not have to just be electronic commerce. The key to electronic commerce and electronic business is that there is a computer or network attached to transactions. Although as Prins specifies, these processes are not completely automated. At some point in the transaction there is a human interaction. These human interactions become important because they often cause the necessity of extra security protocols outside of firewalls and technological controls. The threat posed by human interaction with consumer information is later addressed. (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002)

Electronic commerce can occur between a variety of players. According to Cordy (2003), there are 9 types of interaction. Electronic commerce can occur between businesses and consumers, B2C. This is the type of interaction that this paper explores at length. The next type of interaction is business to business, B2B. The majority of electronic commerce sales occur through this channel, due to the high volume of products that are transferred between companies; supply chain management expresses this relationship. Government is also a large player in electronic commerce, through business to government transactions, B2G. Amazon.com makes consumer-to-consumer transactions easier, C2C. There are also C2B transactions, for when a consumer might want to sell something to a business. Consumers are also able to engage in consumer to government transactions, C2G. An example of such an interaction would be the ability to pay fines online. There is also G2C interaction, government to consumer. This would include things such as renewing a driver's license online. Similarly, the government can interact with business, G2B for permits or other services. Government is also able to interact with other agencies through electronic commerce, G2G. Government can engage in file or information sharing. Transactions of electronic commerce can take various forms, although this paper will focus on business to consumer interactions. (Cordy, 2003)

Benefit to firm:

Although the uses of E-business vary, it is certain that the use of e-business is in the best interest of the firm, as it provides another venue in which perspective consumers can be reached. Initially many firms were hesitant to enter the e-business market due to its novelty, however competition forced them to make their products available online. E-business can make customers more accessible to the sellers. Businesses no longer need an intermediary to conduct business. An example of this would be a clothing store that uses the store as an intermediary between the goods and the customer. For a customer to purchase a good they must go into a store. E-business takes out the physical store and directly connects the goods to the customers. They can select goods online and have those goods shipped directly to their home from the warehouse. From the firms' perspective they are able to cut the cost of supplying the good. They do not have to pay the intermediary costs, such as the sales associates to enable the sale. The cost of delivery itself is passed onto the customer, through shipping costs. Overall the cost of selling the good to the consumer becomes less expensive. (Mann, Eckert, & Knight, 2000)

Not only can the firm save on the cost of the sale but it can also increase their clientele. The ability to conduct commerce online has made the clientele global. Customers can pay to have their goods shipped all over the world. Prins (2002) believes that the market for current goods has expanded, and there is no longer a niche market, but rather a much larger one. In addition to the expansion of current markets there is the ability to make new markets for service or "information-based products". An example of this is when hospitals have the ability to outsource the review of x-rays to other countries. These are all things that can be considered a part of electronic business. (Smith, 2004)

Electronic business is especially lucrative to smaller businesses. Businesses that cannot afford to reach foreign markets are able to do so with electronic commerce. Smaller businesses can easily reach a larger market by setting up a website (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002). They are able to compete with larger companies through e-commerce. The benefits are not only ease of interaction but also the inexpensive cost of transactions. Smaller companies do not need a physical presence to enter a market. They are able to save money by not having a physical store for customers to enter; and can still compete with larger companies. Customers can access catalogs and inventory directly online. (Smith, 2004)

The ability for companies to put their catalogs and inventory online is another way that firms are able to save money. Rather than paying for catalogs to be printed and shipped to potential customers, firms have the option of posting those same catalogs online. Firms can email catalogs out to the customers, which decreases the cost of printing. The cost of advertising is decreased, and the ability to market to customers both domestically and globally increases. (Smith, 2004)

Conducting transactions electronically is quick and less expensive overall. Online the customer has the option to use credit or debit cards as well as online wallets. The money can be taken from the customer and the transaction approved immediately. This cuts down the time between when a sale is made and when the transaction is processed. Another advantage is a reduction in errors made when a transaction is processed. When customers previously called the company to place an order through an operator, errors in orders were more common. The customers can enter information into a sales form themselves, which cuts down on the errors in processing; this saves the business money, as they do not have to pay to correct these mistakes. Whether it is a mistake as to what item is shipped, or if incorrect shipping information is entered when placing an order by phone. These are all areas that can be improved by the use of electronic commerce. There is also a reduction in the errors of electronic business. Enterprise wide systems allowed information to be shared across the firm, reducing redundancies and inconsistencies within the firm. To conclude, the benefits to the use of electronic business are numerous. Businesses are able to store information at a lower cost. There is less need for physical files. There are also fewer receipts and paper storage of information. The move to into E-business has many benefits from firms’ perspective. (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002)

Consumer Benefit:

The benefits to consumers engaging in electronic commerce are similar to those gained by firms. Consumers find that shopping online is more convenient. They do not have to drive to the store, or worry about standing in line to pay at a register. Customers can quickly pick out what they want to purchase and have those purchases delivered to their homes without hassle. Consumers can forgo interactions with fellow shoppers as well as store personnel. They can complete a purchase in less time, than necessary in a store. There is an ease that comes with electronic commerce. There is also a wider variety of products available online. The same sweater will be offered in more colors and sizes online because it is too costly to stock the same variety of merchandise in stores. The next benefit to consumers is that they are able to quickly find items they are looking for, that otherwise might have been unattainable. For example, a rare item or antique can quickly be located online. A product that was geographically out of reach becomes accessible. Consumers can also use the Internet as a way of shopping around; they can research the products they want to buy and find the lowest prices from home. The marketplace that is available to consumers in global, they are not geographically restricted. If a store is not within driving distance the consumer can still reach the seller by using their online store. The consumers enjoy the wide range of accessibility and the ease of use associated with electronic commerce. (Horrigan, 2008)

Current Debate:

As the Internet economy continues to grow, so does the underground Internet economy. The underground Internet economy is used to describe the “economy of hacker, phishers, and scammers”; it is a term that describes the money made by thieves. “Internet Security Company Symantec reported that the nefarious work of cybercriminials has become a $275 million industry, and is most prevalent in the United States”, which represents 41% of this theft. Online crime is becoming larger as the amount of electronic commerce grows. (Slattery, 2008)

It is clear that the firm has a lot to gain from engaging in electronic business. Yet there are many concerns about the sharing of information through a computer intermediary. Firms in the race to bring their companies to the electronic market place took some risk in the formation of their processes and interfaces (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002). One of the largest problems with e-business is the security of information. The question of the security of information is very broad. There is a question of the security of information that is knowingly collected from the customers; the information that the customers enter onto the web interface, as well as the information that is unknowingly collected by the company. Information is collected through cookies or other data mining activities. When the customer allows companies access to their personal information they are taking a risk. They trust the company to protect them, although these companies do not always have their best interest at heart. The purpose of electronic commerce is to increase profits, and not necessarily to protect the consumer. However, the ability for customers to trust companies becomes important because it can limit what customers are willing to purchase online. Trust issues can limit the amount that is spent by customers online. (Horrigan, 2008)

When a customer visits a website, a lot of information can be collected by the operator of that website. Without having to enter information, the website can install a cookie in a browser or even in the user’s hard-drive. The cookie allows the website to save information about the products that a user views, or other websites the user visits. All of the information obtained is compiled and a profile of the user can be created. The cookie has the ability to save consumer preferences as well as target the consumer for more specific marketing campaigns. In a study conducted by Suhong Li (2009), it was found that 78.7% of fortune 500 companies have cookies on their websites. Overall 82% of these companies admit that they collect personal information from their users. Examples of some of the data that is collected includes: name, email address, postal address, phone number, credit card number, social security number, age, family information, gender, education, income, preferences, and occupation. E-businesses today have the ability to collect personal information from their users. Although businesses are the focus of this research, not just businesses have the ability to collect personal data; government and health agencies do as well. The federal government allows citizens to submit their tax returns online as well as other personal data. Hospitals can keep medical records online. These are all examples of the ways in which consumer information is at risk, although this discussion is limited to the ways in which businesses jeopardize personal security.

According to Li (2009),

> “Privacy is the ‘right to be left alone’. As an extension of privacy in the information age, information privacy is the legitimate collection, use, and disclosure of personal information, or ‘the claims of individuals that data about themselves should generally not be available to other individuals and organizations and that, where data is possessed by another party the individual should be able to exercise a substantial degree of control over that data and its use’”. (Li & Zhang, 2009, p. 207)

Today, with the ability of businesses to collect information online, our privacy is constantly at risk. Not only are companies able to collect this data for their personal use, but they can also choose to release this information to third parties. Other parties might be interested in buying a log of the purchasing practices of consumers. The data collected through cookies and other applications allow companies to forecast sales trends and make marketing strategies based on consumer preferences. In many cases, by choosing to engage in electronic business, consumers are subject to the collection of data and are unable to opt out of participation. A number of sites will not operate effectively unless the browser allows the use of cookies. According to the Li (2009) study of fortune 500 companies, only 23% of companies give the consumer the opportunity to opt out of disclosure to third parties. The question then is, “Should consumer have more control of their information?” (Li, 2008)

Trust in Electronic Commerce:

Consumers are lacking control over their own information and are forced to trust firms. The concept of trust is important when it comes to engaging in electronic commerce. Lack of trust can keep a customer from conducting business online. There are various definitions of the “trust” that must be maintained for consumers to feel safe enough to continue business transactions. Luhmann (1988) defined trust as, “a mental mechanism that help reduce complexity and uncertainty to foster the development of the maintenance of relationship even under risky conditions” (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002, p. 17). Another definition of trust in electronic commerce is, “consumers trust online businesses’ impartial goodwill in providing quality services” (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002, p. 17). Impartial goodwill is not to intentionally hurt a stranger. Consumers need to have some type of trust in the organization before they can engage in commerce. They must trust that by putting their information online it will be safe and secure and they will receive the goods they have ordered.

A secure transaction is one in which “two parties have properly authenticated and that the information exchanges via the network remained unaltered”(Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002, p. 13). The customers must have trust in the firm. According to “Trust in Electronic Commerce” the issue of trust is psychological and has been blown out of proportion. It is possible that the trust that consumers feel they are lacking is not inverse to the amount of risk of engaging in electronic commerce. The author, Prins, believes that the media has blown up the issue of security. Stories that show identity theft through online transmission receive attention from the press. The author believes that it is just as easy to copy a credit card number offline, and that traditional credit card use is not more secure. The author however fails to address the greater possibility of theft that is possible through online transmissions. Someone in another country can just as easily access your information as someone standing beside you. Also, online theft can be in larger volumes. A thief doesn’t have to wait to overhear one person at a time; within moments the thief can have hundreds of credit cards numbers and just as quickly use them. Although there is the possibility that consumers are unable to properly perceive risk, which lowers their trust in electronic commerce, the issue of dwindling trust still remains.

If businesses want to maintain and increase business in the future they are forced to increase trust felt by customers online. Consumers do not trust online transactions for a number of reasons. First is “unfamiliar services”; electronic commerce is still a new technology. Second is the “lack of direct interaction”, because consumers cannot see the place of business or the sales person, they cannot use sight to judge safety. Third is that trust is more difficult is because of the “credibility of the information”. In the Internet economy anyone can set up a web address, it can be difficult to differentiate legitimate from fraudulent businesses. These are all reasons that consumers have difficulty trusting online firms. (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002, p. 15)

There are things that firms can do that will make customers trust their site. The first thing that increases customers’ trust is branding. Branding is anything that makes “its company and services known to customers in a way that differentiates them from competitors” (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002, p. 29). Other factors that increase customer trust are: ease of navigation, fulfillment of orders, presentation, up-to-date technology/security, and privacy seals. The most important thing that the company can do to increase the trust it is given by customers is to build its reputation. The reputation of a company plays a large role in trust felt by the consumers. However, there are limits to what the firms can do to gain trust. For example, there are technical limitations to what a company can do; privacy seals are a difficult protocol to enable. The Internet economy is global; as such what is meaningful in one country will not be as meaningful in another country. A privacy seal might be meaningful and enable trust in one country, but in another it could be inconsequential. One of the best ways that customers increase their comfort with an online business is through familiarity. The more a customer uses the site and has had successful interactions with the company, the more they will trust it. This of course will take time but it has a large affect on the trust within the relationship. Trust is an important part of electronic commerce. Relationships will be limited or possibility terminated if trust cannot be maintained. The customer must be able to trust the company with their privacy and security to continue engaging in business with the company online.

Electronic Privacy:

Privacy in today's age is very difficult to achieve, "information is preserved forever in the digital minds of computers" (Solove, 2004, p. 1). Websites are able to collect a wide range of detailed data while using digital dossiers. These digital dossiers can create psychological profiles that can be used to investigate backgrounds of individuals. Companies to make decision on their actions toward the customer use the information collected from digital dossiers. Digital dossiers can be used by companies when deciding whether to engage in business with you, financial institutions; when determining if and how much credit should be extended, employers; who can judge background and decide whether to hire you, and law enforcement; to investigate identity theft. There is a lot of information flowing from the private sector to the government. The government requests such information. An important distinction to make here is that although harm might not be caused to the individual despite the collection of personal information, there is still an invasion. The existence of dossiers creates the possibility of harm. There are benefits to the collection of such data; a bookseller for example can recommend future books that the customer might be interested in buying. Another benefit would be the ability to save data so that information will automatically be entered when prompted. The result of digital dossiers is not always harmful.

The rise of data collection and digital dossiers are results of technology. As technology increased so does the ability to collect and store data. Although demand plays a role in the ongoing supply of personal data, these data exist due to technology. According to Solove, it was the “advent of the mainframe in 1946 [that] revolutionized information collection”(Solove, 2004, p. 14). Then couple that with the rise of the Internet, making information available at everyone’s fingertips. The Internet has become the “hub of the personal information market, it has made the peddling and purchasing of data much easier” (Solove, 2004, p. 22). Every action that a consumer engages in online can be recorded and analyzed for further use by companies, people and government. Technology often presents the possible danger; the best that can be done is to minimize the risk of harm. At current the risks of engaging in electronic commerce continues to grow and there are not adequate security protocols to minimize the growing risk. Personal privacy online means the ability to not have all your actions recorded without giving your permission. Despite the benefits of electronic commerce the questions remain, should the customer be able to opt out of such data collection? Do customers have the right to keep some of their activities to themselves? As Alan Westin says, “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (Solove, 2004, p. 76).

Threats to Privacy:

The most talked about threat to the security of consumers is the possibility of identity theft. There is a possibility that their information could be stolen and thieves could pose as them and engage in fraudulent business transactions. Identity theft can cost the consumer financial damage. Identity theft occurs when the thieves uses personal information such as social security number, name, or credit card information without permission. This is one of the threats of putting your information online. This can occur when the thieves are able to obtain the information through phishing; “consumers receive unsolicited emails requesting information, and they unwittingly provide private information, which is then used maliciously. The theft can also occur when a company does not secure electronic information appropriately or when employees steal the information”(Secor & Tarn, 2009, p. 19). Information can be stolen in a number of ways. Electronic commerce has many points of weakness that thieves can exploit. (Secor & Tarn, 2009)

One of the ways that information can be stolen is during transmission. It can happen through eavesdropping during the communication of the personal information. This can mean simply overhearing the information or it can mean obtaining the information through a network connection. Even if the data is encrypted thieves are able to break the encryption using cryptanalysis. Next, a breach of security can occur when the information is accessed while it is being stored by the business. If a company stores confidential customer information on a network that has an Internet connection it is more vulnerable to attack. Thieves can try to crack the firewall and access the information of many customers, rather than just on a person- to- person basis. The last way that security can be breached is when an authorized party accesses the information. An example of this is when an employee of a firm uses confidential information for personal gain. These are all points of intrusion to personal security. (Prins, Ribbers, Van Tolborg, Veth, & Van der Wees, 2002)

A firm can jeopardize customer security in two ways. Firms can knowlingly walk the line between “privacy and profit” or they can simply unknowlingly cause harm to consumers. Firms that choose to risk the privacy of customers that they interact with choose to sell information for their own gain. An example of this would be the current controversy surrounding companies such as Facebook. Facebook has been accused of selling personal user information to advertiers. Facebook can track navigation and behaviors of their users and then sell the information collected to marketers; from there advertisers can make targeted ads to Facebook users. Facebook benefits from this, as they are paid for user information. This is an example of where companies knowlingly take away personal privacy in favor of a profit. (Swartz, 2010)

Firms can also violate the privacy of consumers unknowlingly. They can unintentionally violate customer information by releasing data in unforeen capacities; where there in no intended malice. An example of a recent violation is with Apple’s iPad, that made AT&T service vulnerable to hackers. The AT&T website that users access made the email addresses of other subscribers unknowlingly avaiblable; making everday citizens as well as prodment political figures volunerable. Once AT&T was aware of the situation, the firm was quickly able to solve the problem, however the invasion of privacy could not be undone. This is an example of how companies can unknownling harm consumers. The company did not mean to violate personal privacy, however through a simple lack of care harm was cauased. Privacy as well as security can be violated both intentionally or unitentionally. Government intervention could help to prevent either type of violation however, similar mistakes cannot be completely eleminated. Government has the ability to change the actions of firms and the motivaton to intervene; firms are seeking profit whereas the government can be a consumer advocate. (Cha, 2010)

Customer Conundrum:

The consumers appreciate the value of engaging in electronic business. The Pew Research Center found that 2/3 of Americans online has purchased a product. One of the largest influencers of whether consumers decide to purchase goods online is their perception of the site. Users want to feel “safe” before they grant businesses access to their personal information. According to Pew, currently 75% of all users say that they do not like to give their credit card information out over the Internet. Pew concludes that whether a customer feels safe sharing information influences what and if they engage in electronic commerce. Pew found that 93% of online users at one point have engaged in electronic commerce. They enjoy the privileges but would also like to curtail some of the risk. To do so, government intervention would be necessary. Horrigan (2008), questions, “why should the government intervene in the dealings of private businesses?”

Incomplete market:

One of the reasons that government should intervene in the dealings of private companies is because the market is incomplete. This means that there is not a free flowing of information between both seller and user. Customers are unaware of their privacy rights. Although most companies do post privacy agreements on their sites, it is unlikely that customers will read and understand them. Another reason that the market is incomplete is because the market does not properly reflect the risk associated with electronic commerce. By allowing companies to access confidential information, the user is putting their information at risk. They are at risk of financial loss, when it comes to the possibility of their information being stolen and used by thieves. They are also at risk for the infringement on their privacy. There is a high transaction cost. The risk to consumers is not reflected in the price that they pay for these online services, and thus the market is imperfect. When a market is imperfect government should intervene to right the market imperfection. In this case the government should evenly distribute the burden of risk on both the firm and the user, both parties that are engaging in electronic commerce. (Mann, Eckert, & Knight, 2000)

Asymmetric Power:

Another reason that the government should intervene in the market is because the firm holds more power than the customer. The customer does not have the ability to tell the firm what information can be collected and how it should be used. The firm has most of the power. Electronic commerce has benefits for both user and seller, although the terms are based on firm wants rather than customer wants. Customers who choose to engage in electronic business lack control over their own information and privacy. Although they authorize the use of information by one company, they cannot stop the information from being transferred to a third party user. (Mann, Eckert, & Knight, 2000)

This imbalance of power is referred to as the “power-responsibility equilibrium”. According to Wirtz (2007), the firm should ensure that consumers feel secure in releasing their information because they have more power in the consumer-firm relationship. Under this model it is in the best interest of the company to make the consumer feel secure in operations, thereby taking responsibility. If the firm does this they are more likely to keep their customers. If this equilibrium is not met, then firms risk losing some of their profitability. Yet, as most online customers feel uncomfortable sharing their information, it is clear that firms left to their own devices are not meeting this equilibrium. (Wirtz, Lwin, & Williams, 2007)

Currently companies are left to decide the best way to protect their customers’ information. The process of deciding what practices should be adopted is subjective. Each company has its own protocol for dealing with security, and there is not a minimum level of security required for websites. Although some companies choose to have third party monitors, there are no protocols for those companies either. According to experts in the field of electronic commerce, there is no standard for “best practices”; government could provide the field with a standard operating procedure to ensure the protection of consumers. (Khosrow-Pour, 2004).

Economic Growth:

A study conducted in 1992 found that 91% of Americans believe that government and businesses are not doing enough to protect the privacy of consumers (Wirtz, Lwin, & Williams, 2007). If the consumers feel that their security is not in jeopardy, then more people would be willing to engage in electronic commerce. If the government is not moved by the outcry of the public for change, then they should be willing to intervene in the market for self-interest. According to Mann, the increased use of electronic commerce could increase GPD by 5% over the next ten years,

> "Electronic commerce increases the efficiency of resource utilization, which translates into faster productivity growth, which supports higher sustained GDP".
>
> (Mann, Eckert, & Knight, 2000, p. 23)

The government should consider intervening in the actions of private firms as a way of increasing the GDP within the United States. Wirtz is not the only believer that electronic commerce is in the best interest of the U.S. economy, as Rob Atkinson believes, "the internet is currently the major driver of economic growth in the U.S." because its growing quickly and has yet to show signs of slowing (Gross, 2008). Electronic commerce is tied to health of the U.S. economy; it is in the best interest of the economy for electronic commerce to continue to grow.

Transparency:

At current, electronic commerce lacks transparency. Consumers are unable to judge the full extent of the risk they face each time they engage in electronic commerce. (Oranje-Nassau, Krapels, Botterman, & Cave, 2009). There is a general sense of risk when engaging in activity online, however on a transactional basis consumers cannot see the risk they face. Not only are the customers unaware of all the ways that they face risk, they also do not know their privacy rights, or if and how their information is being used. Companies should be required to disclose how information is collected, and how it will be used, and the customer should be made aware of this. The government should intervene in electronic commerce to ensure that there is transparency present, and to better allow consumers to judge risk. Transparency in Internet transactions will promote trust in company-customer relationships. Trust is important in e-commerce as a means of encouraging online transactions.

Government Involvement:

Engaging in electronic commerce is the choice of the individual. It is easy to say that customers simply should not conduct business online if they are concerned with security. Consumers need not make this all or nothing decision. Government should act to make electronic commerce safe. In an effort to make electronic commerce safer for consumers, government should enact a law requiring a minimum level of security for electronic commerce to occur between businesses and consumers. At current,

> "The regulatory framework for e-commerce is chaotic: there are numerous international organizations, national government and trade associations producing reports, studies and policies. There is little agreement about the operational details of e-commerce regulation." (Lawton & McGuire, 2003, p. 52)

The federal government can step in and create a standard, at least for businesses within the US that will supersede any state legislation. As the government attempts to regulate electronic commerce they will face difficulties in jurisdiction (Cordy, 2003). The Internet is global, and yet there are no global governing entities (Lawton & McGuire, 2003), making it difficult to resolve disputes. The difficulty in resolving problems should not discourage the government from attempting to solve this complex policy issue.

The government benefits from the growth of the Internet economy. The growth of the Internet economy positively affects GDP and the U.S. economy. As previously discussed, reasons for government intervention include: incomplete markets, subjectivity of security protocols, imbalance of power, economic growth, and transparency. The consumer is unable to judge the risk of electronic commerce and thus is unable to behave according. Consumers also face greater personal risk by engaging in such activity. The government should enter this imperfect market, and although the Internet will never be completely safe, it can be made as safe as possible (Oranje-Nassau, Krapels, Botterman, & Cave, 2009).

Current regulation:

The laws that handle digital privacy and security are inadequate to handle the current electronic climate. According to Solove (2004), there are five different types of regulation aimed at preserving privacy: constitutional law, federal and state statutes, evidentiary privileges, property law, and contract law. A difficulty with the laws currently in place is that they seek to prosecute invasions rather than to prevent violations. Another problem is that invasions are judged separately from one another; each companies’ individual invasion of personal privacy. The real danger however is the result of collective actions. Many dossiers are able to form full profiles of people. It is difficult to enforce privacy statues when you do not know whom to blame, because the real threat is collective. When some companies obtain your name and personal information and another company can obtain your purchasing history the combination of data profiles create a threat to personal privacy.

At current there is a lack of legislation regulating electronic commerce. There is an entity specifically set up to handle complaints against unfair practices, identity theft, and privacy issues. This agency is the Federal Trade Commission (FTC), and more specially the Division of Privacy and Identity Protection. Consumers can file complaints with this agency, and have those complaints forwarded to the appropriate judicial entity. Although this agency is charged with handling consumer complaints, the best they can offer is suggestions for consumers as to how they can protect their information. The Division of Privacy and Identity Protection is limited in what they can enforce. They can only enforce three acts: the first being section 5 of the FTC Act that prevents the deceptive use of consumer information. Although the FTC has this power, and consumers can file complaints, it is very difficult to obtain proof. As Solove states,

> “Many modern privacy problems are the product of information flows, which occur between a variety of different entities. There is often no single wrongdoer; the responsibility is spread among a multitude of actors, with a vast array of motives and aims, each doing different things at different times.”

It is difficult to pinpoint a single person that is responsible for customer privacy violations. Another power of the FTC is that they can entice companies to adapt privacy agreements to protect consumers, by exerting pressure publically and calling attention to current practices. Upon completion of this voluntary agreement, the FTC can then prosecute companies that violate this agreement.

Research Questions:

The research questions posed in this study are:

- How do selected members of the RIT community use electronic commerce
- What level of trust do these members of the RIT community have in electronic commerce
- What changes in regulation of electronic commerce would these members of the RIT community like to see

RIT is used as a case study to provide insight into current experiences with e-commerce from populations that are likely to have high levels of engagement in online activity. The purpose of posing these questions is to see if there is a difference in the way that two groups use electronic commerce, and if this difference in use affects trust and experiences. Another insight to be gained is measure the trust in electronic commerce, and to gauge how much this population would like to see a change in regulation.

Chapter 3

Methodology

This paper further investigates the use of E-business by average Americans. I further explore the opinions of Americans in addition to what was gained through Pew Research data. Information on usage, experiences, and ideas for the future was collected. In addition to these goals, I was able to draw limited generalities regarding the sample populations. The data were collected through the use of a patchwork design. Various data collection methods were combined in order to achieve this goal. The benefit of patchwork design is to gain validity (Bingham & Felbinger, 2002). Some of methods that were used include: Case study design, Post-test only comparison and survey techniques. “Case study is not either a data collection tactic or merely a design feature alone but a comprehensive strategy”(Yin, 1994, p. 13), in combination with other techniques, patchwork design represents an appropriate method for data collection.

Case Study:

The subjects of the case study are faculty and students at Rochester Institute of Technology. Case studies were conducted at the university to gauge the experiences of the RIT community. The comparison groups are faculty at Rochester Institute of Technology and students at the university. The RIT community is likely to engage in electronic commerce due to the university’s culture of technology use and innovation. This case study measures the extent to which members of the community engage in electronic commerce; some of their experiences, their feelings of trust in the activity, and what involvement they would like to see from the government. Rochester Institute of Technology was chosen due to convenience and the willingness of respondents to complete the survey.

Additional boards other than the Institutional Review Board (IRB) were not necessary to conduct the research. The research was also inexpensive to conduct on the university campus. Another benefit to conducting the research at RIT is that the RIT population is expected to be highly likely to conduct business online because of the university’s heavy emphasis on technology and computing. Computers and Internet access are readily available to the entire population on-campus, increasing the likelihood of use. Increased use affected the amount and depth of the data collected.

Two groups were surveyed for comparison. The first are professors teaching in the College of Liberal Arts (COLA). Rochester Institute of Technology is home to 8 colleges within the university. The College of Liberal Arts was selected because it has the largest faculty among the university’s colleges. The College has approximately 164 faculty members, of which there were 36 responses. The comparison group that was asked to complete in the survey was students currently enrolled in liberal arts classes. Students in three Sociology classes were asked to complete the survey, and 90 responses were obtained. The classes were introductory level courses, representing a diversity of undergraduate majors. The total number of students within the university is 14,045 undergraduates.

The faculty population is an appropriate sample group due to the diversity of backgrounds. This group is also preferred because of the limitation in sampling the general population. Also, faculty within the Rochester area are more likely to engage in the electronic commerce according to the Pew Center, which described the characteristics of those that engage in electronic commerce. The Center found that the greater the educational attainment, the more likely people are to engage in electronic commerce. The Pew Center described this variable as “college +”. Professors are a part of this category due to education level required to teach. The age range for professors will vary which will show the experiences of varying age groups as well as whether opinions will vary based on the age of the participant. Professors are also likely to engage in electronic commerce because of their income. The portion of the population who earn under $40,000 a year is less likely to engage in electronic business. Due to their high average income, professors are expected to highly engage in electronic commerce. Studying faculty and students at RIT was a convenient and inexpensive way to collect data on the use of business technologies, consistent with (Horrigan, 2008, p. 8). Choosing this population specifically increased the likelihood that the participants would complete the survey.

The basic research employed was a case study, which was convenient and minimized cost. It benefits the study in that it allows a large amount of descriptive data to be collected. According to Schramm (1971),

> “the essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a decision or set of decisions: why they were taken, how they were implemented, and with what result” (as cited in Yin, 1994. P12).

An instrumental case study was employed in this study. One subgroup is examined in order to make more general recommendations about the population (Stake, 1995). In addition to being an instrumental case study in practice, in implementation it was a collective case study. There were multiple case studies conducted to add to the validity as well as to provide some comparison. This is how the post-test comparison research design was implemented. The case study was conducted at a single period in time. The difficulty with doing case study analysis is that it is harder to make generalizations across a larger population, “Our obligation is to understand this one case” (Stake, 1995, p. 4). Although by doing a collective set of case studies, I hope it will better allow generalities to present themselves.

According to Yin (1994), before a case study can begin, a number of steps that must occur:

1) Define the case study question- what will the case study answer? Why are you conducting the study? List advantages of using the case study to answer the question.
2) Define the “significant” questions to be answered by the case study- three major questions. How would your findings influence the field?
3) Identify “significant” questions in other research methods- identify if there are other methods that could answer the questions you view as significant.
4) Examine other case studies- Look at other case studies to see if there is something to be gained and applied to your research
5) Define the different types of case studies- look at the various types of case studies that can be conducted.

The steps above are all recommended to the researcher before he begins the case study (Yin, 1994, pp. 16-17). Theses steps will be later addressed within the section.

Survey:

Data were collected through the use of survey techniques. A written survey was given to participants for completion. A mixture of multiple choice and open-ended questions was asked, allowing both qualitative and quantitative data to be collected. Both of the case study groups were given the same survey, and it was only given at one point in time. The goal of this study is to gauge the use of Internet technologies; there will not be a series of studies conducted over a period of time. Given the time limitation of the study, multiple surveying times were not feasible, in contrast to collecting the changing levels of trust. The survey sought to answer the questions posed by the case study.

“A survey can be defined as a focused, organized means of data collection”(Angrosino, 2002, p. 136). The purpose of using a survey is that a lot of data can be collected very quickly. The survey allowed for more participants to engage in the case study, had other techniques been used for data collection the case study would have to limit the number of participants. According to Angrosino (2002), survey research is:

1. Logical- it will yield results that can be objectively shown
2. Determinist- can show casual links
3. General- applicable to larger populations
4. Parsimonious- can collect data on a number of questions
5. Specific- there is a specific way of measuring relationships

A survey more clearly answers the research questions posed in this paper, including questions as to current usage, knowledge of the data being collected, trust in electronic commerce as well as what the community would like to see in the future.

According to Babbie (1973), the purpose of conducting a survey is to describe the population, explain the relationships between parties, and explore new relationships (Angrosino, 2002, p. 137). The survey given to both populations includes descriptive questions to gauge income, race, and sex. These questions determined whether general data collected by the PEW Research Center also fit with the RIT community. The survey also explains feelings that online customers have toward both government and companies by asking open-ended questions. These questions asked participants what they felt the role of each party should be. The survey explored new relationships by asking the participants what they would like to see in the future from all of three party (customers, companies, and government) in the future to protect both security and privacy.

Surveys can either be cross sectional or longitudinal. The difference in these two forms of survey is the number of times the surveys are administered. The survey used in this study was cross sectional, in that it was administered a single time. Also, the purpose of the study is to describe the population and explain the actions of the population at a single point. A cross sectional survey best achieved this research goal.

When conducting research it should be new, it should add to the community and not restate commonly accepted truths. As such Angrosino (2002) has a guide to the questions that are posed to the participants. The questions should not have already been answered in the field. The questions should shed new light on old assumptions. Lastly the survey should help to understand current problems. This survey differed from many surveys in that it mixed both closed and open-ended questions, so that greater information can be collected concerning the population. Also, most of the research done in the field was in general terms and did not seek to conduct a case study of a specific group. The survey was kept as short as possible so that the respondents were more willing to complete it in its entirety. The design of the survey is adapted from surveys from Wirtz, Pew Research Center and Prins (2002).

Other surveys have been done in the field of electronic commerce, what makes the survey here different is that one specific group of people are being tested. The goal of this survey is not to generalize across a larger population; it is a case study. The first survey from which I was able to pull a number of questions is the Wirtz (2007) survey. The hypothesis being tested with this survey is whether customers perceived privacy is influenced by what the customers believes the companies' privacy and security protocols are. Some of the sections covered in this survey are: privacy concerns, responses to concerns and demographic questions. Many of the questions that I ask relating to consumer trust of electronic commerce are largely based on the Wirtz survey. The Wirtz paper did not include the results of the survey specifically, but rather offered up lessons learned. Wirtz found that when the customer does not feel comfortable entering information they either choose to discontinue the sell/interaction or choose to enter incorrect data. As a result marketing data quality suffers. The results also showed that consumers would like to see government and organizations protect their privacy.

The next paper that was influential in choosing which questions to ask in the RIT case study was published by the Pew Research Center. This survey was influential in asking questions of how respondents use electronic commerce. The difference between the Pew survey and the RIT survey is that the goal of the RIT survey would like to go further and not just ask if respondents have ever used electronic commerce in a facet, but how often the respondent uses electronic commerce in that facet. The last survey that was influential in the survey process is the Prins survey. The Prins survey also played a role in the trust section of the RIT survey. The RIT survey asked more questions of trust and also allowed the respondent the opportunity to answer open-ended questions. The RIT survey is different because first it is a case study of one specific group and does not attempt to generalize across a larger population. It is also more advanced than other surveys previously conducted because the respondents are able to give more open-ended responses, which allow for greater detail of opinions and occurrences. A reason for this difference in form can be largely attributed to size; the other surveys were given to thousands of people. The RIT survey was done on a much smaller scale, which allows for greater insights and details from respondents.

Questions were asked to the participants in three categories: usage, trust and population characteristics. The first category is the usage category, and it is meant to provide understanding regarding what faculty and students believe to be electronic commerce. The questions asked under this category can be seen in Appendix A1 for faculty and A2 for students, although for this category the questions posed to each group is identical. The first question asks if the participant has Internet access at home. The purpose of this question is to see how much access the respondent has to Internet. Also, this characteristic can be measured against other questions to determine if those who have Internet access at home are more likely to engage in electronic commerce. This question is multiple-choice and can be described as nominal. The two possible answers are not related to one another. This type of question can also be described as a forced choice question. The next four questions are all forced-choice questions with ordinal answers. Ordinal answers are ranked in relation to one another. In this case the question is asking about frequency of use, the first answer is daily, and the answers that follow decrease in relation to one another. The next possible answer after daily is weekly followed by monthly, rarely and never. The first five questions under the usage category all lead into the sixth question. The five priors were organized as such, so that the respondent would understand the sixth question. The question of how often respondents engage in electronic commerce is dependent on their answers to the previous questions, that all specifically reference electronic commerce activities. The last two questions in the usage section are open ended. The first asks the respondent to detail any other activities he or she believes to be electronic commerce, so that there is a better understanding as to what faculty and students view as electronic commerce. The final question in the section asks why respondents choose to engage in electronic commerce. Previous research states the reason for engaging in electronic commerce is convenience, lower cost, and greater selection. The purpose of this question was to see if consumers have other reasons for choosing to engage in electronic commerce that have not already been discovered. The first section of the survey answers the first research question of how the RIT faculty and students use electronic commerce.

The next section of the survey evaluates the level of trust held by RIT faculty and students in the protection of their privacy and security in the use of electronic commerce. The question asked in the trust question can be seen in Appendix A1 and A2 for faculty and students. All the questions in this section are forced response questions. One difference in this section is that the choice of responding with "I don't know" becomes an option. The purpose of adding this response to the questionnaire is to provide an option when the respondents do not have the knowledge to answer the question.

> “As the object of the questions gets further from their immediate lives, the more plausible and reasonable it is that some respondents will not have adequate knowledge to base an answer or will not have formed an opinion or feeling.”(Fowler, 1993, p. 76)

If the respondents do not have the necessary knowledge to answer any of the questions in this section they are able to select the “I don’t know” forced response.

The next section is the Future section. This section responds to the final research question, “what changes do faculty and staff want to see in the regulation of electronic commerce?” This section is a mixture of both closed and open-ended questions to best judge who Rochester teachers believe should be response for the safety of consumer information and privacy. The purpose of including open-ended questions in this section is so that respondents are given room to explain what they would like see from government, companies and users in the future. The respondents were not biased by forced responses answers, and were able to express themselves more completely.

The final section includes population characteristics. These questions were placed at the end of the survey so that if the respondents were uncomfortable with answering these questions they had already completed the rest of survey. If these questions were placed at the beginning of the survey it could have discouraged participation. Participation in this survey was optional. The purpose of these questions is to understand more about the survey respondents. These general questions were the only identifying characteristics asked of the respondents. The character questions asked of the respondents can be seen in Appendices A1 and A2. These questions allowed for further analysis of the populations. Questions in the categories of usage, trust, future and population characteristics make up the survey.

Human Subjects:

The survey was approved by the Institutional Review Board (IRB). The purpose of this board is to “protect the rights, safety, and welfare of the people who take part in research. The focus of an IRB is to make sure that the risks posed to research participants are justified by the potential benefits”. The survey was submitted to the board for approval before it could be distributed to participants. The board ensures that minimal risks are posed to participants. There is no risk posed to participants in this survey. The board also ensures that privacy is not violated. The respondents in this study maintained anonymity by not attaching their name to the survey. The board also makes sure that the researcher is given the consent of the participants to use their information. In this study, attached to each one survey was a consent form informing participants that their participation is optional, they can stop at any time, and confidentiality will be maintained. This form can be found in Appendix B. The survey was approved and found that the risk to participants was minimal. It was then distributed to respondents.

Goal:

The goal of the case study is to evaluate the experiences of the RIT community with Electronic Commerce. Significant questions that the case study addressed are: How much the RIT community uses electronic commerce? What is the level of trust held by the RIT community in regards to electronic commerce? What changes does the RIT community want to see in the regulation of electronic commerce? The survey poses questions within these three fields. The goal is to obtain some of the personal experiences that faculty and students of RIT have during the use of electronic business. The method of research and analysis as described above are a patchwork design that includes case study research, survey techniques, and a post-test comparison methodology.

Limits:

There are a number of inherent limits to what can be done through case study. For example, “the researcher will uncover more variables than he or she has data points, making statistical control an impossibility” (Garson, 2002, p. 139). Despite the survey including both closed and open-ended questions, it will be difficult to transform the data that is collected into quantitative form. Another inherent limit of conducting a survey is the biases, such as non-response. Participants were not forced to take part in the survey. Other biases included are cultural bias; because of the area that the study was conducted, it is difficult to make generalities. Although there are a number of limits to conducting the study given the time, location, and cost constraints the patchwork design is appropriate to answer the posed questions.

Another limit of the case study is the number of people that were surveyed. For the results to have statistical significance to all of RIT more data would have to be collected. Due to time and resource limitations a sample of this size cannot be collected. The drawbacks of the small sample size are important when conducting statistical analysis. The amount of analysis that can be done with the information collected is thus limited, and open to criticism.

Pre-Testing:

After the completion of the survey it is important to conduct a pre-test. The purpose of the pre-test is to ensure that the questions asked are clear and receive the type of response sought. During the pre-test not only are these participants to complete the survey but they are also to rate the questions and critique clarity, grammar and provide other criticisms of the survey. A pre-test is a way of making sure that the intended recipients understand the survey. When conducting a pre-test, it should be administered under “realistic” conditions to a population similar to the intended population. As such, I chose to pre-test staff and a few students at the Rochester Institute of Technology. Ten surveys were distributed and eight were completed. After conducting the survey, a number of grammatical changes were made and the order of some of the forced-choice answers was re-organized. Also, a benefit to conducting the pre-test is that I was able to banish some preconceived notions that I had concerning electronic commerce. I assumed that most people used electronic commerce to buy things online, however based on the pretest I was able to see that most people used electronic commerce for financials reasons. Meaning, that the majority of the participants used electronic commerce to pay bills online, and everyone used electronic commerce to engage in online banking. Pre-testing is an important part of the surveying process, as it is an opportunity to make further improvements. (Fowler, 1993)

Distribution to Professors:

To distribute the surveys to professors I sought approval from the Senior Associate Dean of the College of Liberal Arts to put a survey along with a consent of participants form in professors’ mailbox within the college. I was approved to distribute hardcopy surveys to all COLA professors. Along with the survey materials, there was inter-office envelopes attached, which encouraged the participants to return the survey to Professor Foltz. The survey was distributed on Friday, April 9, 2009, and requested that it be returned by the following Friday, April 16, 2009. This gave the professors a full week to complete the survey and return it.

Distribution to Students:

To distribute the surveys to students I sought the approval of three professors at the university who were willing to give out a paper version along with a consent of participants forms to students within their classes. Each professor was informed that the survey would take about ten minutes to complete, and asked if they would be willing to distribute the survey during class time. The students in turn would receive the survey and complete it without having to give up any personal time to do so. The survey was distributed to the students with the consent form that informed them that there was no risk to take the survey and that participation was voluntary. No additional information was given to the students, and the topic was not discussed before the survey was taken as to avoid tainting the results in any way. The professors that agreed to have their class participate were asked to distribute and collect the survey at any time during the class period over a week’s time.

Chapter 4

Results

RIT professors returned a total of 35 surveys. In contrast to the students population there was a much larger turnout. Of the three classes that were visited I was able to obtain a total of 85 Student surveys. A more specific description of the results is to follow. Each of the questions asked will be explored to see what can be learned from the responses of each group. The responses solicited from both groups within the Rochester Institute of Technology will be compared with some of the data found from previous studies in the field of electronic commerce.

The following table (Summary of Results Table) shows the results of the surveys given to both professors and students. The table reveals the median response of each group, and specific results will be discussed following the table.

Summary of Results Table

Questions	*Median Professor Response*	*Median Student Response*
Do you have Internet Access?	Yes, 88.6% (31/35)	Yes, 98.8% (84/85)
How often do you buy items online?	Monthly, 57% (20/35)	Monthly,48% (41/85)
How often do you pay bills online?	Monthly, 48.6%(17/35)	Rarely, 20% (17/85) 39% responded Monthly
How often do you engage in online banking?	Monthly, 34%(12/35)	Weekly, 82.9% (29/35)
How often do you use amazon.com?	Rarely, 47% (16/34)	Rarely, 42% (36/85)
How often do you engage in Electronic Commerce?	Rarely, 41% (14/34)	Rarely, 36.5% (31/85)
How concerned are you with the possibility of identity theft?	Somewhat, 65%(22/34)	Somewhat, 66%(55/83)
Do you believe when you enter your personal information online it will	Yes, 58% (19/33)	Yes, 57% (46/81)

Are you aware that banks or shops can keep records about your payments when you use debit cards and other electronic payment systems?	Yes, 97% (32/33)	Yes, 91% (77/85)
Are you aware that companies can track which purchases you make and which websites you visit without your knowledge or permission?	Yes, 84%(27/32)	Yes, 69%(59/85)
How often do you use false or incomplete data when registering for a site to maintain personal privacy	Rarely, 12%(4/34) Bi-modal Sometimes, 44%(15/34) Never, 41%(14/34)	Sometimes, 55%(47/85)
Is it important that no traces are left of your electronic payments like name, bank account, or address?	Yes, 88%(29/33)	Yes, 68% (57/84)
Are you comfortable sharing your personal information online? (Examples: name, address, credit card number, phone number, etc.)	No, 62% (21/34)	No, 55% (46/84)
Have you had any negative experiences regarding electronic commerce?	No, 80% (28/35)	No, 80% (66/83)
Would you stop using a system if you feel it’s not trustworthy?	Yes, 94% (32/34)	Yes, 95%(81/85)
Do you wish you had greater control over what information is collected by companies?	Yes, 94%(32/34)	Yes, 94% (80/85)
Do you believe there should be tougher regulations by government to protect personal privacy online?	Yes, 61% (20/33)	Yes, 76% (64/84)
Age?	Average: 50	Average: 20
Race?	White, 79% (26/33)	White, 84% (70/83)

Income?	60-100K	40-60K

The survey contained three sections, usage, trust and future. The results from each of the sections will be further discussed below.

Usage:

Do you have Internet access at home?

In regard to the questions concerning use, the first question asks the respondents if they have Internet access. The vast majority of both professors and students have Internet access at home. Between the two populations, a larger proportion of students have Internet access at home in comparison with the professor population. According to census data in 2000 only 41.5% of American homes had Internet access. While time has surely increased the number of homes having Internet, the RIT population itself is more likely to have Internet at home due to the institute’s emphasis on technology.

How often do you buy items online?

Students and professors had similar responses to the question of how often they buy items online, choosing a median response of monthly. However this becomes interesting if you combine all those that responded: daily, weekly, monthly, and rarely, indicating that they have bought an item online. All professors at one time have bought an item online, and 98% of the students at one point have purchased an item online. This same question is asked by the Pew Research Center; only the center found that only 66% of Internet Users have purchased an item online. The number of RIT respondents who have made online purchases is significantly higher.

How often do you pay bills online?

There is a significant difference in the median responses from professors versus that of what students said. The median response from students found that students rarely pay bills online. However, the distribution for students is bi-modal; about half of the respondents never pay bills online, while the other half monthly pay bills online. A display of this distribution can be seen in Figure 1. A reason for the difference could be the number of bills held by each party; the age difference may play a role in the difference between replies.

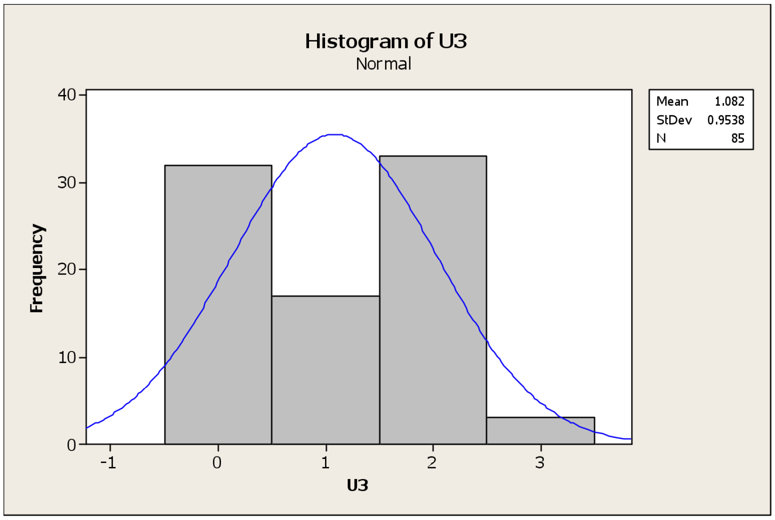


Figure 1: Frequency of students paying bills online

How often do you engage in online banking?

RIT students engage in electronic banking more often than RIT professors. However, if responses are combined to reflect all those who have ever engaged in online banking the statistics for both groups is more similar; 83% of professors and 82% of students. In comparison to research done by Pew Center, RIT engages in online banking more so than the average population at only 53%.

How often do you use amazon.com?

Both groups have similar responses to this question, and rarely use amazon.com.

How often do you engage in Electronic Commerce?

The median response to this question by both groups is rarely. However, it can be assumed that the neither population full understood the question. The definition of electronic commerce was clearly defined before the sections yet respondent were confused by this question. A respondent that said they bought items online monthly, responded that they never engage in electronic commerce. To calculate the percent of all those who have ever engaged in electronic commerce returned the following results: 85% of professors and 87% of students. This is an inaccurate tally of those who have engaged in electronic commerce. If the same summation is done with buying items online then it is found that 100% of professors and 98% of students at one point have purchased items online. In comparison to what Pew found 93% of Americans engage in activities that are considered electronic commerce. Despite the inaccurate response, the majority of RIT students and professors engage in activities related to electronic commerce. It can be assumed that despite the Institute's focus on technology, neither population has a clear view of what activities are considered electronic commerce; therefore users underestimate use.

Overall, the data collected in this section can be used to answer my first research question: How do RIT professors and students use electronic commerce. It can seen through this data that a greater portion of professors use electronic commerce to pay bills online. They also engage in online banking in a less frequent manner. Students on the other hand are more likely to use electronic commerce to conduct online banking, on a weekly basis.

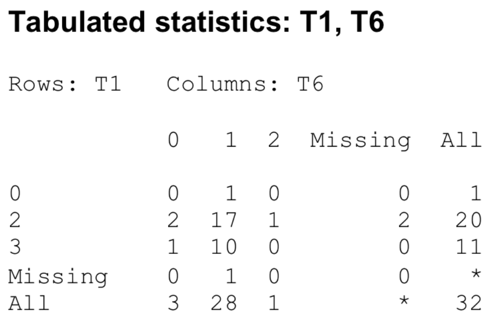
From the open-ended questions I was able to learn more about motivations for the two populations to engage in electronic commerce. As previous research has found, a large reason for engaging in electronic commerce is convenience. Other previously predicted reasoning includes, a large selection, speed and cheaper goods. Other reasons provided by the respondents are, the saving of postage when mailing bills, ability to read online reviews and the ability to do fast comparison-shopping. These are all reasons that professors gave for choosing to engage in electronic commerce. Students at RIT provide similar responses, with one addition. Students believe that the use of electronic commerce is beneficial to hard-of-hearing students; electronic commerce eliminates the communication barrier present in many physical stores. This is a response that is the result of the community studied, because RIT has a partnership the National Institute of the Deaf.

Also asked in an open-ended format, other activities the two populations viewed as electronic commerce. Some of the responses solicited from professors are, donating, eBay, Craig's list, paying dues to professional organizations and publication processing. For the most part however professors did include other activities they viewed as electronic commerce. Students too had other activities they view as electronic commerce. One of the main addictions to the list of activities constituting electronic commerce is social networking, using sites such as Facebook. Other activities students believe to be electronic commerce are, emailing, buy music, and paying for online services (gaming). All of the above activities fit within electronic commerce. The usage section of the survey answered my first research question of how each population uses electronic commerce.

Trust

How concerned are you with the possibility of identity theft?

The two populations come to a consensus that they are somewhat concerned with the possibility of identity theft with 65% of professors and 66% of students believe this. What is more interesting is that the people that are either somewhat or very concerned about their identity theft, find it important that no traces are left of them online. Those who are concerned with identity theft do not like to have a large presence online. 84% of the professors, who were somewhat and very concerned with identity theft, were not comfortable with traces being left of them online, along with 61% of students felt the same way. The results of these calculations can be seen in Figure 2 and Figure 3.



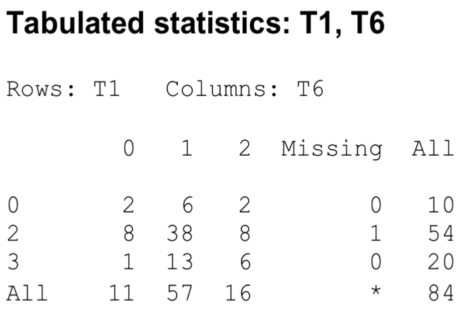
Tabulated statistics: T1, T6

```
Rows: T1    Columns: T6

             0   1  2  Missing  All

0            0   1  0        0    1
2            2  17  1        2   20
3            1  10  0        0   11
Missing      0   1  0        0    *
All          3  28  1        *   32
```

Figure 3: Professors. T1- ***How concerned are you with the possibility of Identity theft?*** **T6-** ***Is it important that no traces are left of your electronic payments like name, bank account, or address?***



Tabulated statistics: T1, T6

```
Rows: T1    Columns: T6

          0   1   2  Missing  All

0         2   6   2        0   10
2         8  38   8        1   54
3         1  13   6        0   20
All      11  57  16        *   84
```

Figure 2: Student.T1- ***How concerned are you with the possibility of Identity theft?*** **T6-** ***Is it important that no traces are left of your electronic payments like name, bank account, or address?***

Do you believe when you enter your personal information online it will be protected?

The median respondent in each group believed that their information would be protected. Though, it was interesting to see how respondents that had their information stolen would respond to this question. Professors whom had negative experiences concerning electronic commerce, responded that they were did not know if their information would be protected. In contrast to the students that had their information stoles. Those who had negatives experiences were split; some felt their information would not be protected while others still believed their information would be protected. Those who’ve had negative experiences with electronic commerce respond in different ways.

Are you aware that banks or shops can keep records about your payments when you use debit cards and other electronic payment systems?

In response to this question 97% of professors responded that they are aware, while 91% of students said they were aware. In comparison to the general population, RIT is more aware of companies are doing with customer information. In comparison with data collected through the Prins’ survey, concluding that only 60.5% of the sample population was aware of these practices.

Are you aware that companies can track which purchases you make and which websites you visit without your knowledge or permission?

The median response for both groups was yes, however, a larger majority of professors where aware of this practice than students.

How often do you use false or incomplete data when registering for a site to maintain personal privacy?

Students more often than professors enter false information online. The median student enters false information, sometimes, while the median professor enters false information rarely. However, the distribution of professor responses is more bi-modal. Professors either enter false information never or sometimes. A graphical display of professor response can be seen in Figure 4. The reason for this difference could because of the different in the way that they use electronic commerce. Professors may be using more reputable sites. However, it is clear that students enter false information more often than professors. Professors either enter false information on a more regular basis, or abstain from the practice.

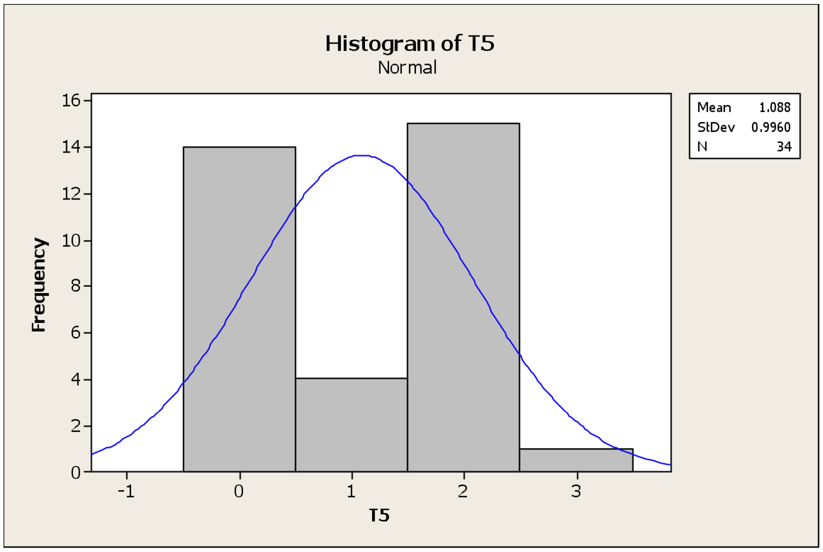


Figure 4: Professors that enter false or incomplete information

Is it important that no traces are left of your electronic payments like name, bank account, or address?

The median response from each group is, Yes.

Are you comfortable sharing your personal information online?

“Internet Economy: Should the Federal Government Intervene?”

The median response from each group is, No.

Have you had any negative experiences regarding electronic commerce?

The vast majority of respondents believed that they had never experienced anything negative while conducting business online. Out of the 35 professors that responded, only 7(20%) indicated that they’d had a negative experience regarding electronic commerce. Of the 83 students that replied, 17(20%) indicated they’d had a negative experience. This is much lower than I would have expected. Also, a possible reason that this number could be underestimated is because some will not classify as experiences as negative. For example, if a large company does not fulfill an order, and yet the customer is able to recover any losses; the customer will less likely to classify the experience as negative. Also, respondents might not want to admit to any ignorance on their own part. Of those that detailed the negative experiences, some examples are: stolen identity, stolen credit/debit card, products that never arrived, products that were misrepresented online, purchases items that could not be returned, and spam. If negative experiences are not an underestimation, we can assume that because RIT has a higher technical training the community is better able to protect itself.

Would you stop using a system if you feel it’s not trustworthy?

Both groups responded, Yes; 94% of professors and 95% of students. This is very similar to the survey in Prins; 94% of the respondents would stop using the system. In this case the RIT population is very similar to general population.

After garnering all the responses under the Trust category of the survey I am able to answer my second research question; what is the level of trust held by RIT students and professors concerning electronic commerce. It can be said that RIT has a higher level of knowledge concerning the practices of companies and firms electronically. Along with this knowledge comes unease with entering personal information online. Yet, in contrast to this unease both populations believe their information will be protected. This shows the conflicting beliefs of the population. Though they know information is being collected and are not comfortable with volunteering their information they are putting trust in the system to protect them. Those who have had negative experiences are unsure as to whether their information will be protected. Despite knowledge of misdoing, the RIT population has trust in electronic commerce.

Future:

Do you wish you had greater control over what information is being collected by companies?

The median response from respondents is, Yes.

Do you believe there should be tougher regulations by government to protect personal privacy online?

The median response from both professors and students is, Yes.

When each group was asked whom they believe should be in charge of personal privacy, students believed that, you (the consumer) should be responsible followed by companies that you give your information to. Professors however believed that companies should be primary responsible, consumers secondarily.

The next question that I asked of respondents was what they believed that customers could do to protect themselves from invasion of privacy and security. Professors and students had similar responses to this question. Both groups believed that consumers to protect their information could do the following things:

- Hire personal protection agents
- Beware of the vendors they use; only use "legitimate sites"
- Don't give out any extra information that is not required by the site
- Use secure sites/transactions
- Minimize online activity or don't engage in online activity
- Delete cookies
- Use strong passwords
- Read privacy statements
- Don't click online ads
- Have a credit card specifically for online transactions

When respondents were asked what they believe companies can do protect the personal privacy and security of their customers. To this the groups respond:

- Be responsible for what is done with collected information; don't sell it.
- Use strong security protocols
- Limit the length of time that customer information is stored

- Only collect necessary customer information
- Not release customer information without explicit permission to do so
- Give customers the ability to "opt out" of data collection
- Better data encryption

Lastly, under the future category the respondents were asked what government could do to protect the privacy and security of online customers, to which they respond:

- Regulate security protocols of companies
- Monitor companies more closely
- Prosecute violations
- Make law to keep companies from selling information without consent
- Stronger regulation of electronic commerce
- Give security software to companies
- Create government version of Paypal

All the above suggestions were a synopsis of what RIT professors and students would like to see in the future from customers, companies, and government to protect security and privacy of electronic commerce. These responses answer the question of what RIT would like see changed in the regulation of electronic commerce. However, what both groups have to remember is that although they would like to see companies work on their own to make electronic commerce safe for customers is unlikely to happen. Companies often are unwilling to engage in extensive self-regulation due to the cost of security advances. To adopt further security would increase cost to the company, in contrast to the ultimate goal of increasing profits. For companies to have strong security protocols they need an incentive to do so, this will come in the form of further government regulation. For companies to behave in a manner to protect personal security and privacy would require the government to not only create laws to govern the companies, but also follow through with strict enforcement. The consumer can do little things to protect himself or herself, it is up to government to force companies to behave in a vigilant manner.

Although students believed customers should be responsible for protecting themselves, it is clear from their own recommendations that companies have the most power to protect them. It is companies that can increase security and not sell information. Though, it is government that is most willing to protect consumers and can force companies to make positive changes for privacy and security. Students charge the person with the least power, students, to take responsibility. Professors on the other hand believe that companies should be responsible, yet they lack the motivation to protect customers. Though the RIT population has an idea of how they’d like customers, companies and government to behave they do not have a grasp on the power and motivation of each group.

Chapter 5

Discussion

After conducting a case study of RIT students and faculty it can be seen that both groups have similar usage, trust, and thoughts on the future of electronic commerce. However, in comparison to the general public RIT is more knowledgably concerning practices of companies online, and also engage in electronic commerce on a more regular basis. This conclusion is based on the comparison of the survey results to previously conducted research. Although, these RIT professors and students trust that their information will be protected, they both have reservations about entering such a vast amount of personal data online. As such, they would like to see companies take more care in dealing with personal security and privacy.

Though the data collected cannot be used to generalize across the U.S. or even the entire RIT population, the data collected is useful. From the data collected I have found that professors in the College of Liberal Arts, and their students have similar concerns over their personal security and privacy. Many of their actions and concerns are similar. However, there is some variance in the way in which they use electronic commerce. It seems that Professors more often are online to pay bills, and conduct more professional business. Where as students use electronic commerce as a way of conducting social networking and the check their bank balances. This reflects the difference in generations that is outlined in Pew Center research. Pew found that younger boomers are more likely to engage in activities such as email, research, obtaining news, making travel arrangements, buying things online and more serious activities, as compared with Generation Y which is more likely to use the Internet for social networking and entertainment activities. My research shows that students (Generation Y) and Professors (Younger Boomers) at RIT follow the same patterns as the general population as defined by Pew. Students are also more likely as a whole to enter incorrect information; assuming due to the less reputable sites that students are willing to visit. Though as a whole the RIT community is more likely to engage in electronic commerce do to environmental influences of the university.

Yet another difference between the two groups is who they should be most responsible for protecting the personal information of consumers. It can be assumed that the reason that Professors believe that companies should be more responsible for customer information is because professors (Younger Boomers) are more like to use reputable sites, in contrast to students. Students (Generation Y) are more likely to search for bargains online according to Pew, which leads them to make sacrifices in the reputation of the sites. This difference can be attributed largely to age; the average age of professor respondents is 50, and the average age of student respondents is 20. Largely respondents were white males for students and professors were largely white, with a nearly even split of women and men. The largest difference between the two groups is level of education and age. Despite these differences the two groups have similar experiences and opinions of electronic commerce.

Recommendations

For companies to take greater care requires government involvement to provide an incentive to companies to behave. Currently, the best way for a customer to protect their personal information online is to simply not engage in electronic commerce. Government involvement could make it safer for customers to have an online presence. A way for government to make it more secure for consumers is to provide greater regulation over companies. There are a number of regulations that government could make in the interest of personal security and privacy.

1. Government can regulate security protocols, requiring all companies online to have a minimum level of encryption or minimum levels of security surrounding the storage of customer information. The will help prevent hackers from obtaining information during the storage stage as well as during transmission. It will make it more difficult for outside hackers to obtain personal information. This will help protect personal security of information.
2. Government could also force companies to make their privacy statement more visible and ensure that site visitors are aware of what information is collected, and what happens with any information obtained. This would help the customers choose whether or not they want to interact with each website. It gives the customers a chance to protect themselves from privacy intrusion.
3. To go further, the government could require the “opt-out” option; any customer that doesn’t want their information shared can prevent a company from doing so. This would help minimize the treat posed when multiple companies come together to create profile of specific consumers. This allows the customer to still conduct business through the site, but gives them greater control over where their information goes and how it is used.

Beyond the regulation is **enforcement**; the FTC currently is limited due to the lack of regulation. If the government decides to add regulation this will require an expansion of the FTC personnel, so that the organization can more quickly prosecute violators. Despite what regulatory action the government decides on, it will necessitate enforcement.

Conclusion

The government should intervene because it is what is in the best interest of the citizens. At current citizens are unable to defend themselves against companies because of their lack of power. Companies dictate relationships with their customers, as such are able to take advantage of the customers. Government has the ability to protect consumers, and is not guided by profits motivation. As shown by RIT respondents as well other studies security and privacy are concerns of the customers. Government has the ability to address such concerns of the public.

There are limits to the survey that was collected. The largest limit of the study was the inability to generalize the results. The results of the case study done at RIT do not represent the general American public. The behaviors of this group are unique to the environment. The number of responses was another limit to the survey; the sample size especially for professors was very low. Low response affects the validity of any statistical analysis, which limited the amount of analysis that could be done. Another limit to the study is that the respondents might not have fully understood each question causing an underestimation of usage or experiences. Similarly, what some judge as “negative” is very subjective causing a difference in responses. The survey conducted in this paper has a number of limits, though general information can be gained.

Through the survey it is clear that the respondents did not feel comfortable entering their personal information online. These feelings were shown to not necessary have come from negative experiences, given that a very small portion of respondents reported negative experiences regarding electronic commerce. To go forward with research involving customers and electronic commerce, respondents should be given a chance to state what they believe to be the best approach for addressing their trust issues. Though they were given a chance in an open-ended format to express their call for action of companies and government, I think that specific policy options would provide better guidance to policy officials. Another question that could be asked of customers is what types of precautions they current take to protect them, to learn more about usage and trust. Overall, the results of the survey were successful in answering the research questions of this paper.

There are a number of takeaways from the case study. In regards to usage, an overwhelming majority of the RIT community engages in some form of electronic commerce. Though, based on age the frequency of engagement as well as the type of engagement varies. The more mature population will use electronic commerce for more business practices, such as paying bills or dues online. The younger generation uses electronic commerce for more personal reasons including online banking and social networking activities. Under trust, it is clear that although people continue to engage in electronic commerce they do not feel comfortable entering their information. However, once information is entered customers are trusting companies to protect them. Looking forward the RIT community would like to see companies work to better protect customer information by instituting higher security protocols and giving customers the opt out option. When companies are unable to volunteer, professors believe that government can establish regulation to promote compliance. The case study allowed for the answering of all the research questions posed by this paper and gave some insight into what customers of electronic commerce would like to see to improve the security and privacy of their personal information.

References

Angrosino, M. V. (2002). *Doing Cultural Anthropology: Projects for Ethnolographer Data Collection.* Prospect Heights, Illinios : Waveland Press.

Bingham, R. D., & Felbinger, C. F. (2002). *Evaluation in Practice* (Second Edition ed.). New York, New York: Seven Bridges Press.

Cha, A. E. (2010, June 12). Apple’s iPad security breach reveals vulnerability of mobile devices. The Washington Post. Retrieved from http://www.washingtonpost.com /wp-dyn/content/article/2010/06/11/AR2010061106239.html

Cordy, E. D. (2003, March). The Regulation of E-Commerce Transactions. *Journal of American Academy of Business, Cambridge* , 400-407.

Fowler, F. J. (1993). *Survey Research Methods.* Newbury Park, California: Sage Publications, Inc.

Garson, G. D. (2002). *Guide to Writing Empirical Papers, Theses, and Disserations.* New York, New York: Marcel Dekker, Inc.

Gross, G. (2008, April 25). Internet Economy Looks Strong, Some Experts Say. *IDG News Service* , pp. 1-2.

Horrigan, J. b. (2008). *Online Shopping: Online Users like the Convenience but Worry about the Security of Their Financial Information.* Pew Research Center. Washington, D.C.: Pew Internet & American Life Project.

Khosrow-Pour, M. (2004). *E-Commerce Security: Advice from Experts.* Hershey , PA: CyberTech Publishing .

Lawton, T. C., & McGuire, S. M. (2003). Governing the Electronic Market Space: Appraising the Apparent Global Consensus on E-Commerce Self Regulation. *Management International Review , 43* (2003/1), 51-71.

Li, S., & Zhang, C. (2009). Chapter XIII: An Analysis of Online Privacy; Policies of Fortune 100 Companies. In K. Chen, & A. Fadlalla, *Online Consumer Protection: Theories of Human Relativism* (pp. 269-283). Hershey, PA: IGI Global.

Mann, C., Eckert, S., & Knight, S. (2000). *A Policy Primer: Global Electronic Commerce .* Washington, DC: Institute For International Economics .

Oranje-Nassau, C., Krapels, J., Botterman, M., & Cave, J. (2009). *The Future of the Internet Economy: A Discussion Paper on Critical Issues.* The Netherlands Ministry of Economic Affairs. The Netherlands: Rand Europe .

Prins, J., Ribbers, P., Van Tolborg, H., Veth, A., & Van der Wees, J. (2002). *Trust in Electronic Commerce.* The Hague, The Netherlands: Kluwer Law International.

Secor, A. M., & Tarn, J. M. (2009). Chapter II: A Taxonomic View of Comsumer Online Privacy Legal Issues, Legistlation and Litigation. In K. Chen, & A. Fadlalla, *Online Consumer Protection: Theories of Human Relativism* (pp. 16-32). Hershey, PA: IGI Global.

Slattery, B. (2008, November 24). The Underground Internet Economy is Alive and Well. *PC World* , p. 1.

Smith, G. E. (2004). *Control and Security of E-Commerce .* Hoboken, New Jersey: John Wiley & Sons, Inc. .

Solove, D. J. (2004). *The Digital Person: Technology and Privacy In The Information Age .* New York, New York: New York University Press .

Stake, R. E. (1995). *The Art of Case Study Research.* Thousand Oak, California : SAGE Publications Inc. .

Swartz, J. (2010, June 15). Facebook walks tricky line weighing privacy vs. profit. USA Today. Retrieved fromhttp://www.usatoday.com/tech/news/2010-06-16 facebook16_CV_N.htm

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern . *International Journal of Service Industry Management , 18* (4), 325-348.

Yin, R. K. (1994). *Case Study Research: Design and Methods* (Second Edition ed.). Thousand, California: Sage Publications Inc.

Appendix A1

Usage

[Electronic commerce is any transaction of information, data, products and services using online communication]

Please Circle Your Response

1) Do you have Internet access at home?
   - a. Yes
   - b. No

2) How often do you buy items online?
   - a. Daily
   - b. Weekly
   - c. Monthly
   - d. Rarely
   - e. Never

3) How often do you pay bills online?
   - a. Daily
   - b. Weekly
   - c. Monthly
   - d. Rarely
   - e. Never

4) How often do you engage in online banking?
   - a. Daily
   - b. Weekly
   - c. Monthly
   - d. Rarely
   - e. Never

5) How often do you use amazon.com?
   - a. Daily
   - b. Weekly
   - c. Monthly
   - d. Rarely
   - e. Never

6) How often do you engage in Electronic Commerce?
   - a. Daily
   - b. Weekly
   - c. Monthly

d. Rarely
e. Never

7) Are there other activities that you engage in online that you would consider electronic commerce?

____

____

8) How do you benefit from the use of electronic commerce?

____

____

Trust

Please Circle Your Response

1) How concerned are you with the possibility of Identity theft?
a. Very
b. Somewhat
c. Not at all
d. I don’t know

2) Do you believe when you enter your personal information online it will be protected?
a. Yes
b. No
c. I don’t know

3) Are you aware that banks or shops can keep records about your payments when you use debit cards and other electronic payment systems?
a. Yes
b. No
c. I don’t know

4) Are you aware that companies can track which purchases you make and which websites you visit without your knowledge or permission?
a. Yes
b. No
c. I don’t know

5) How often do you use false or incomplete data when registering for a site to maintain personal privacy?
a. Never
b. Rarely

c. Sometimes
d. Often

6) Is it important that no traces are left of your electronic payments like name, bank account, or address?
a. Yes
b. No
c. I don’t know

7) Are you comfortable sharing your personal information online? (Examples: name, address, credit card number, phone number, etc.)
a. Yes
b. No
c. I don’t know

8) Have you had any negative experiences regarding electronic commerce? If so, please detail below:
a. Yes
b. No

9) Would you stop using a system if you feel it’s not trustworthy?
a. Yes
b. No
c. I don’t know

Future

1) Do you wish you had greater control over what information is collected by companies?
a. Yes
b. No
c. I don’t know

Please circle all that apply
2) Who do you believe should be responsible for protecting your personal information?
a. You
b. Companies you give your information to
c. Third party companies that obtain your information
d. Government

“Internet Economy: Should the Federal Government Intervene?”

3) Do you believe there should be tougher regulations by government to protect personal privacy online?

a. Yes
b. No
c. I don’t know

4) What do you believe consumers can do to personally protect their own security and privacy online?

5) What should companies do to address both the security and privacy of online customers?

6) What would you like to see Government do to better protect Personal Security and Privacy?

Population Characteristics

1) Home Zip Code

Please Circle Your Response

2) MALE or FEMALE

3) Age ___________________________

4) Race

a. White
b. Black
C. Hispanic

D. Other

5) Household Income

a. 25K-40K
b. 40K-60K
c. 60K-100K
d. Over 100K

Appendix A2

Usage

[Electronic commerce is any transaction of information, data, products and services using online communication]

Please Circle Your Response

1) Do you have Internet access at home?
    a. Yes
    b. No

2) How often do you buy items online?
    a. Daily
    b. Weekly
    c. Monthly
    d. Rarely
    e. Never

3) How often do you pay bills online?
    a. Daily
    b. Weekly
    c. Monthly
    d. Rarely
    e. Never

4) How often do you engage in online banking?
    a. Daily
    b. Weekly
    c. Monthly
    d. Rarely
    e. Never

5) How often do you use amazon.com?
    a. Daily
    b. Weekly
    c. Monthly
    d. Rarely
    e. Never

6) How often do you engage in Electronic Commerce?
    a. Daily
    b. Weekly

c. Monthly
d. Rarely
e. Never

7) Are there other activities that you engage in online that you would consider electronic commerce?

8) How do you benefit from the use of electronic commerce?

Trust

Please Circle Your Response

1) How concerned are you with the possibility of Identity theft?
a. Very
b. Somewhat
c. Not at all
d. I don't know

2) Do you believe when you enter your personal information online it will be protected?
a. Yes
b. No
c. I don't know

3) Are you aware that banks or shops can keep records about your payments when you use debit cards and other electronic payment systems?
a. Yes
b. No
c. I don't know

4) Are you aware that companies can track which purchases you make and which websites you visit without your knowledge or permission?
a. Yes
b. No
c. I don't know

5) How often do you use false or incomplete data when registering for a site to maintain personal privacy?

a. Never
b. Rarely
c. Sometimes
d. Often

6) Is it important that no traces are left of your electronic payments like name, bank account, or address?

a. Yes
b. No
c. I don't know

7) Are you comfortable sharing your personal information online? (Examples: name, address, credit card number, phone number, etc.)

a. Yes
b. No
c. I don't know

8) Have you had any negative experiences regarding electronic commerce? If so, please detail below:

a. Yes
b. No

____

____

9) Would you stop using a system if you feel it's not trustworthy?

a. Yes
b. No
c. I don't know

Future

1) Do you wish you had greater control over what information is collected by companies?

a. Yes
b. No
c. I don't know

Please circle all that apply

2) Who do you believe should be responsible for protecting your personal information?

a. You
b. Companies you give your information to

c. Third party companies that obtain your information
d. Government

3) Do you believe there should be tougher regulations by government to protect personal privacy online?
a. Yes
b. No
c. I don’t know

4) What do you believe consumers can do to personally protect their own security and privacy online?

5) What should companies do to address both the security and privacy of online customers?

6) What would you like to see Government do to better protect Personal Security and Privacy?

Population Characteristics

1) Major

Please Circle Your Response

2) MALE or FEMALE

3) Age ____________________________

4) Race

a. White
b. Black
C. Hispanic
D. Other

5) Joint Parental Income

a. Under 25K
b. 25K-40K
c. 40K-60K
d. 60K-100K
e. Over 100K

Appendix B1

Consent of Participants

Hello! I'd like to thank you for taking the time to consider taking part in my survey. Participation is optional, and you may at any time stop without penalty. Also, if you are uncomfortable with any question posed you may leave it blank. The purpose of this survey is to answer three questions in regards to professors within the Rochester Community:

- How do you use electronic commerce?
- What is your level of trust in electronic commerce?
- What changes would you like to see in the regulation of electronic commerce?

Some of the questions asked of you will concern whether or not you choose to shop online or pay bills online. There will also be a few open-ended questions that ask about other activities you choose to engage in online. The data collected from the survey will be used to draw generalities concerning professors in the Rochester Area. Any information that is recorded on the survey will be anonymous, as I ask that you not put your name on the survey. Also, myself, the researcher, will be the only one to see the survey. None of the surveys will be referenced specifically but rather will be examined as a population. An example of statistics that will be pulled from the data is, 25% of respondents choose to engage in electronic commerce once a month. All of the information collected will be solely for academic purposes.

The purpose of collecting this data is to be used and analyzed as part of a Master of Science thesis in Science, Technology, and Public Policy at the Rochester Institute of Technology. There is no risk to participating in this survey, and it will take under twenty minutes to complete. Your participation would be greatly appreciated if you so choose to complete the survey to follow. If you have any concerns about the completion of this survey please feel free to contact me at sxb6615@rit.edu.

Thanks Again,

Sha'Kera Bumbray

Please return your completed survey via inter-office mail by April 16, 2010, using the attached envelope, to: Franz Foltz 01-1356.

Appendix B2

Consent of Participants

Hello! I'd like to thank you for taking the time to consider taking part in my survey. Participation is optional, and you may at any time stop without penalty. Also, if you are uncomfortable with any question posed you may leave it blank. The purpose of this survey is to answer three questions in regards to students attending Rochester Institute of Technology:

- How do you use electronic commerce?
- What is your level of trust in electronic commerce?
- What changes would you like to see in the regulation of electronic commerce?

Some of the questions asked of you will concern whether or not you choose to shop online or pay bills online. There will also be a few open-ended questions that ask about other activities you choose to engage in online. The data collected from the survey will be used to draw generalities concerning students attending RIT. Any information that is recorded on the survey will be anonymous, as I ask that you not put your name on the survey. Also, I will be the only one to see the survey. None of the surveys will be referenced specifically but rather will be examined as a population. An example of statistics that will be pulled from the data is, 25% of respondents choose to engage in electronic commerce once a month. All of the information collected will be solely for academic purposes.

This data is to be used and analyzed as part of a Master of Science thesis in Science, Technology, and Public Policy at the Rochester Institute of Technology. There is no risk to participating in this survey, and it will take under twenty minutes to complete. Your participation would be greatly appreciated if you choose to complete the survey. If you have any concerns about the completion of this survey please feel free to contact me at sxb6615@rit.edu.

Thanks Again,

Sha'Kera Bumbray