The Ethics Of Data Privacy In An Electronic Marketplace: The Incorporation Of Fair Information Practice Principles Into Privacy Policies

Rochelle A. Cadogan, Ph.D. (E-mail: racadogan@viterbo.edu) Viterbo University and Capella University

Abstract

Electronic commerce will be pivotal to the economy in the current information age. With the dawn of electronic commerce, some consumers have become concerned about the disclosure, transfer, and sale of information that businesses have collected about them. These concerns allegedly are slowing the rate of expansion of electronic commerce, consequently putting the future growth of the New Economy at risk. This research project is a multiple case study of the incorporation of Fair Information Practice Principles in the privacy policies of three online organizations: Amazon.com, Dell.com, and PrivacyAlliance.org. While many individuals prefer anonymity, most are willing to give out their personal details in order to receive some service or product. The majority of consumers take offense when their personal information is mistreated. However, what is the right way to treat personal information? What should be the foundation of a good privacy strategy? How does an organization promote trust in their data practices utilizing a privacy policy notice? How does the privacy policy disclosure effectively incorporate notice, choice, access, and security—the four key elements of fair information practices? The purpose of this study was to investigate these questions. This study focuses on the market for personal information used for advertising and marketing purposes. This market is affected by most of the regulatory and legislative proposals now under consideration. While much of the research is focused on electronic information gathered over the Internet, the analysis applies to off-line information as well. Additionally, recommendations for future research in the areas of data privacy based on information discovered in this project are identified in this paper.

1. Introduction

The chief executive officer of Sun Microsystems said in early 1999 that consumer privacy issues are a "red herring." "You have zero privacy anyway," Scott McNealy told a group of reporters and analysts in January 1999 at an event to launch a new technology product. "Get over it," he added.

McNealy made the remarks in response to a question about what privacy safeguards Sun would be considering for Jini. The Jini technology is designed to allow various consumer devices to communicate and share processing resources with one another.

"Get over it." Most consumers would be uncomfortable with those words coming from a person of authority in the information technology industry. Consumers have an expectation that industry leaders such as McNealy would propose solutions to enhance citizen privacy rather than just telling them to "get over it." McNealy's comments came only hours after competitor Intel reversed course under pressure and disabled identification features in its Pentium III chip.

Jodie Bernstein, director of the Bureau of Consumer Protection at the Federal Trade Commission, said that McNealy's remarks were out of line. Bernstein also stated that millions of American consumers express serious concern regarding privacy and shopping online (Sprenger, 1999).

Readers with comments or questions are encouraged to contact the author via email.

Two and one-half years later, the Sun Microsystems CEO is saying that "absolute privacy is a disaster waiting to happen" (McCullah, 2001). McNealy (2001) is convinced that we have barely scratched the surface on this one. He feels that someday soon you could find yourself in a strange city and your Web-enabled wireless phone will be able to recommend a nearby restaurant based on your fondness for French, Italian or Mexican cuisine—and then make a reservation for you. It could even recommend a movie based on what you liked and did not like in the past—and, by the way, it is playing three blocks away, starts in half an hour and only a few tickets are left, so would you like to purchase one now with your credit card?

According to McNealy (2001), these are just two examples of how specific needs will be met in specific circumstances and many more are possible. McNealy believes that the point is, for that level of service, most people would gladly reveal their personal preferences, as long as they feel certain the information will not be misused. And, on the Internet, even more than in other areas of our lives, trust is the real currency. "Squander what you have and you'll find out how hard it can be to get more" (McNealy, 2001).

It is McNealy's opinion that, up to this point, the industry has done a pretty good job of regulating itself. Most companies now post formal privacy policies on their Web sites and allow visitors to have a say in how information about them is used.

According to Kincaid (2001), surveys show that almost 40 percent of individuals who bought online last year agree that privacy concerns kept them from shopping again, and nearly 60 percent express concerns about companies selling their information to third-parties. Kincaid states that privacy concerns are not going away so e-commerce companies should get over that!

With increasing consumer concerns about the privacy of personal information, privacy is very much on the minds of businesses across many industries. Organizations who turn privacy into an advantage by successfully adapting their organizations to address the growing concerns will be successful. By earning consumer trust and taking advantage of the information that consumers share, organizations will be in a wonderful position to benefit themselves and their customers, concurrently. Consumers want to know that information will not be circulated without their permission and this is the foundation of building trust. In the growing world of the online marketplace, the protection of consumer information should be a primary concern and a joint effort between consumers and organizations.

Privacy has been a hotly debated topic in Washington and other national capitals in the Information Age. The debate over privacy has spawned an astounding assortment of industry and academic conferences, working groups, public interest and lobbying efforts, public surveys, and news stories. However, results from this research study provide additional feedback that confirms that consumers are generally not knowledgeable in this topic.

The recent high volume of attention to privacy is an outcome of the rapid spread of information technologies in every facet of life and the popularity of the Internet. Remarkable increases in computing power and dramatic decreases in the physical size and price of computers have produced an online environment in which both individuals and organizations increasingly use computers, producing unparalleled growth in and reliance on computer-facilitated services, and resulting in greater demand for and use of computers. Currently organizations utilizing the virtual storefront business model face a wide range of privacy concerns, expressed by customers. One outcome of Internet usage is that more data than ever thought possible will be made available in digital format. This is significant since digital information is easier and less expensive than non-digital data to retrieve, manipulate, and accumulate—especially from separate and geographically isolated locations. Additionally, our information technologies and services tend to record what could be described as superfluous data, such as the Web sites we have visited.

As a result, others know more about consumers—each of us—than ever before. Some of this data is information that you might not even know about yourself. The ramifications of such a readily accessible repository of electronic information are astonishing.

Most major Web sites now have privacy policies which detail how the organization collects and uses personal information gathered from visitors. The government has pushed for these types of policies and organizations hope that if sites post them voluntarily, Congress will not intervene and pass restrictive privacy laws.

The complexity of organizations, such as the three organizations investigated in this study (Online Privacy Alliance, Dell, and Amazon.com), account for the complexity of the privacy policies. The complicated issues do not have straightforward solutions. According to Christine Varney of the Online Privacy Alliance (OPA), existing protections for personal health and financial information, as well as the protection of personal information about children, are being implemented by the government and industry. Varney suggested, in a Senate Commerce Committee Hearing on Privacy, that it is appropriate to wait until gaps in these protections develop (2000). However, do consumers want to wait?

The topic of this study is critical. Advances in information technology have made it possible for comprehensive information about consumers to be compiled and shared very easily and inexpensively. In certain aspects, this is positive for society. For example, it is easier for law enforcement personnel to locate criminals, for banks to prevent fraud, and for consumers to learn about new products and services, which allows consumers to make more intelligent purchasing decisions. Simultaneously, as personal information becomes more accessible, businesses, associations, government agencies, and consumers must take precautions to protect themselves against the misuse of that information.

2. Fair Information Practice Principles

A multiple case study, which examined the incorporation of Fair Information Practice Principles into three privacy policies, was utilized in this research study. Multiple sources of evidence provided for a thorough analysis of privacy policies of three very distinct organizations. Although the organizations selected for this study contrast in their business models and missions, all share a concern and a respect for customer data. Due to this common thread, the conclusions of this study may have a more general applicability to understanding privacy policies and the value of Fair Information Practice Principles than what could have been predicted before the initiation of this study.

Concerned about the exponential growth of the online consumer marketplace and the capacity of the online industry to collect, store, and analyze vast amounts of data about consumers visiting commercial web sites, the Federal Trade Commission (FTC) reported in May 2000 on its most recent privacy survey of commercial web sites. The survey's objective was to assess the online industry's progress in implementing four fair information principles which FTC believes are widely accepted. They can be defined as follows:

1. Notice. Data collectors must disclose their information practices before collecting personal information from consumers.
2. Choice. Consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided.
3. Access. Consumers should be able to view and contest the accuracy and completeness of data collected about them.
4. Security. Data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use (FTC, 2000).

This multiple case study has provided a depth of information and analysis into the "ethics of data" and the incorporation of the four fair information practice principles (notice, choice, access, and security) into the privacy policy disclosure of three vital online organizations in today's information economy. As the opportunities and technology to use personal data for personalized, targeted marketing grow, organizations need to strive for striking a balance between delivering targeted marketing of products and services and preserving the privacy that consumers expect. Organizations must develop effective policies that walk the delicate line between using data to provide services without violating privacy. Consumers demand it and organizations must educate themselves in how to provide services without the violation of consumer privacy. Organizations have vital reasons to take the privacy balancing-act very seriously. The time is now for organizations to gain the trust of consumers because there is no doubt that these consumers are extremely concerned about the privacy of their personal information.

It is a new day and age. Privacy will be to the information age economy what consumer protection and "Save the Earth" concerns have been to the industrial society of the 20th century. Is there a better way to deal with this newness than to begin with education? Education is the critical resolution to the widespread access to information and knowledge sharing—organizations, and consumers alike, would benefit from a focus on education into the "ethics of data" and fair information practice principles.

This paper will focus on the following vital topic areas relating to privacy policies and the "ethics of data" based on the findings of my research study:

1. Information as an Asset—Past and Present
2. Opt-in versus Opt-out
3. Enriched Data
4. Readability and Contradictions
5. Benefits versus Concerns
6. Children's Privacy
7. The Future of Information Privacy

Additionally, recommendations for future research in the areas of data privacy based on information discovered in this project are identified in this paper. The suggested topic areas for future study and deliberation, which will be expanded upon later in this paper, include the following:

1. Cyberterrorism and Privacy
2. Identity Theft
3. Effectiveness of Privacy Protection Technologies
4. Learning from the Gramm-Leach-Bliley Experience

With a better understanding of the necessary components of trust-earning privacy policies, organizations can more effectively provide what consumers demand in regards to adequate protection of their data. The risks are enormous in the online environment. The failure to respond appropriately to privacy issues and risks can result in adverse consequences that range from outright market rejection to regulatory enforcement action, to loss of data flow, or to costly litigation. We must begin by understanding that, for the organization, information is an asset—and has always been an asset.

3. Information as an Asset—Past and Present

When a consumer purchases groceries at a supermarket, the information needed to process the credit card transaction is not the only information that passes through the checkout stand. The popular supermarket discount club, Sam's Club, creates a record of every item purchased, combining the information scanned from the items at the register with the person's identifying information in the store's computer. The supermarket can use this information to create coupons instantly to entice someone who likes Kellogg's corn flakes to try the house brand instead.

Why is so much information collected about everyone's daily purchases? The reason is that information is power in the Information Age. The laws of economics in the Information Age center around the fact that information has value—it is a product that can be sold, just as any other product on a store's shelves.

In addition to stores using information about consumer purchases for their own marketing, the information is often sold to other businesses or to agencies that package it and sell it to other direct-mail marketers. While the compiling and use of mailing lists are not new, modern database and datamining technology makes consumer data a much more valuable product because it can sort, select, and customize it in so many ways. For example, a catalog company can target just those women who might be interested in purchasing children's clothing.

Now, add the Internet to this—already existing—data sharing economic environment. In many ways the Internet is a shopper's dream come true. By surfing the Web, a consumer can obtain detailed information on almost any product or service and quickly shop for the best price available. Items can be ordered with a credit card and a few keystrokes. A good example of shopping with minimal keystrokes is Amazon.com's 1-Click Shopping. The Internet has become a billion-dollar market with millions of customers buying items online utilizing minimal keystrokes.

However, the Internet also adds another way to scoop up huge amounts of information from and about consumers during these transactions. Many Web sites, including two of the three studied in this research project, store an identification file called a "cookie" on the Web surfer's hard disk. They can then combine that information with the Web server's log of all the Web pages the user views. The result is a detailed profile of what the customer had bought—and is likely to buy. The cookie file can save the customer time (by making it unnecessary to resubmit credit card and address information for each order) and can be used to "customize" the site with the consumer's preferences and to offer shopping suggestions, as Amazon does. On the other hand, the information can be used to generate spam (electronic junk mail) or it can be sold to other marketers (creating more spam).

E-commerce can assist in individualizing and personalizing customer relations. The Internet allows for bi-directional communication because e-commerce businesses can directly observe visitors to their Web sites by registering the clickstream (the trail of mouse clicks made by a user during Web surfing) of the visitor. Additionally, e-commerce organizations can request that visitors to their Web sites complete a registration form, which usually includes questions about the customer's social and economic background. Collecting and processing customer information can serve as an important factor in competition. Online organizations can inform their customers individually of updates or complementary and related products, and products can be specifically assembled according to the customer's interests—such as with online newspapers or investment recommendations. The present behavior of the individual online customer can be compared with the behavioral patterns of typified customer groups and service can be adapted accordingly. A simple example noted in my study is Amazon.com's book recommendations. When you buy a book, you learn of additional books purchased by customers who also bought the same book that you purchased. This concept is based on the notion that since both you and Charlene bought the same book that you have the same interests. Therefore, if Charlene bought an additional book, you would want to know what book she purchased. The premise of this marketing concept does have some merit and individual privacy is not violated. In this study, many suggestions that have been offered to me by Amazon.com were useful suggestions. Yet, this tactic presents some restrictions. Amazon.com has started to sell do-it-yourself tools and equipment on its Web site. With Amazon.com's tactic, buyers of a drill could be informed that other buyers of the same drill had also purchased the DVDs of the Hollywood films "Apocalypse Now" and "Titanic". What is the relationship between a drill and the movie "Titanic"?

Detailed knowledge regarding customer preferences is an important asset for e-commerce organizations. However, organizations need to be cautious when using the word "asset" according to David Zapolsky, Associate General Counsel for Amazon.com. Zapolsky comments that if Amazon.com would have the opportunity to revise their privacy policy again, this time they would not use the term "assets" when referring to the data they have collected from users of their online corporation. Traditionally, it is well understood and expected that customer information is normally transferred in mergers and acquisitions of businesses or business units. These transfers are common in today's corporate environment. According to Zapolsky, no one has ever suggested that, in the Warner/AOL merger, the Time or People magazine subscriber lists or the pay-per-view movie purchase history of cable customers should somehow be immune from transfer to the combined AOL/Time Warner entity. To the contrary, subscribers are more likely to be concerned with ensuring continued and timely service—something that is impossible to achieve without customer information.

So, why the media frenzy when this change in the privacy policy incorporated the term "assets"? It appears that a lack of education on the part of the consumers is a key reason for all the media attention. Privacy groups can frighten the consumer who does not understand that in the legal landscape of a business acquisition or merger, customer data is an asset. The online environment does not change that fact—information has always been an asset. However, the relative newness of the online environment provides an open field for creation of fear and some privacy advocates have taken advantage of this consumer uneasiness.

4. "Opt In" versus "Opt Out"

One of the questions concerning the use of personal data is whether consumers should have to request becoming a data subject (opt in) or request to be removed from any data list (opt out). Currently, it appears that most companies rely on the opt-out approach.

It can be argued that it would be better for both companies and consumers to adopt the opt-in model. This would permit businesses to better target consumers, while individuals would be better enabled to avoid invasion of

their privacy. Opt in would prevent consumers from being inundated with mail they do not want and for which they are sometimes charged by their service provider.

A number of resources in this study took a different view, suggesting that opt in is an impractical approach from a marketing standpoint and would be excessively costly for industry. The comment was made by several participants in this study that the "opt in versus opt out" discussion ignores the fact that information about consumers has already been captured before anything is purchased. By providing a response on a Web site or by simply visiting a Web site, consumers are actually opting in—unknowingly in many cases.

As the research in this study has revealed, the consent argument may be the most debatable question of this entire issue. Some organizations think the opt-in choice makes it overly burdensome for consumers to gain access to a site. Opt-in supporters say opt-out gives companies too much latitude to generate verbose privacy policies that make it difficult for consumers to truly understand what is actually being done with their personal data.

Organizations doing business online using the Internet have strong business interests in fulfilling the privacy desires of consumers, to the extent those wishes are strongly discernible in their purchasing decisions and consumers are aware of the content of their personal information that may be released to other parties. Could it be possible that if organizations participating in the electronic marketplace used opt in, they would be perceived as being more trustworthy? Generally, the evaluators who participated in this research study felt more comfortable with an opt-in option.

5. Enriched Data

Consumers want to know what type of data might be provided from a third party that is used to enhance or merge with the original personal data. The result of enhancing or merging data from a third party with information provided by the consumer provides what is referred to as "enriched data." Additionally, consumers will want to know if this enhanced and merged data will be accurate data. If online retailers are to continue to exist—and flourish—it will be due, in part, to the emergence of improved technology that helps them to better track consumers' surfing and purchasing behavior better and to create profiles that are more easily shared among marketers. However, the innovations with the purpose of keeping online retailing flourishing also jeopardize it. These capabilities have produced a powerful consumer criticism from an increasingly technical-savvy public. Consumers are stepping up demands for control of their personal data and accountability from the organizations that have it.

Many consumers believe that the use of enriched data presents a significant privacy threat. Web sites are upgrading their customer databases with information from other online companies, and even employers and charities. It is possible that this rich data could be inaccurate and trying to control it is very difficult.

In this study, Amazon.com and Dell utilized the concept of enriched data. Dell states the fact very clearly in its privacy policy: "Dell may enhance or merge your information collected at its site with data from third parties for purposes of marketing products or services to you." Is it upsetting that Dell.com combines your personal data with some (undefined) third party data to provide better service to you? How does the customer feel about this? Opinions seem to vary. Is it upsetting—or only good business sense—that Amazon.com keeps track of its most popular selling books, CDs, and videos by city (and even by the organization where the buyer is employed)? Again, it depends on whom you ask. Some consumers do not have any problem with this tactic; others find this activity to be a violation of consumer privacy. The evidence discovered in this study verified that consumers had differing opinions.

6. Readability and Contradictions

Do the organizations providing privacy policies want the reader to understand what they are telling you in the policy? Mark Hochhauser, the psychologist and linguistics expert who has analyzed many privacy policies, feels that policies are cumbersome and full of jargon. An analysis of the Web sites identified in this study also identified some concerns in readability. If you really do not want people to understand the policy, write it in legalese and have it run on for four or five pages was Hochhauser's (2001) comment.

Readability problems caused by poorly written privacy notices are common in areas outside of the Internet, as well. In the process of research gathering in this study, another privacy policy debate was evident. Beginning in the year 2001, banks and other financial institutions have begun to inform their customers about their privacy rights. The federal Financial Services Modernization Act, also known as Gramm-Leach-Bliley (GLB), requires customers to be offered the choice to opt-out of their bank's sharing of personal information with third parties. Privacy notices were mailed to consumers in their bank statements, credit card statements, investment reports, mortgage statements, insurance mailings, and other financial statements during the summer of 2001. This was a requirement of the new regulation and follow-up distribution of privacy policies is required, as well.

Hochhauser (2001) reviewed 60 of these financial privacy notices using several software programs. These programs calculated the Flesch Reading Ease Score, writing style, sentence and vocabulary complexity, and word commonness. According to the results, instead of being written in plain English, the 60 privacy policies average a 3rd-4th year college (grade 15.6) reading level, making them "difficult" to read on the Flesch Reading Ease Score. In short, average readers will find these notices hard to understand, those readers who are elderly and whose primary language is not English will have even greater difficulty.

Hochhauser (2001) states that recent Census data shows that about 85% of adults have a high school degree. About 25% have one or more college degrees. Despite these levels of educational attainment, research shows that many people read three-to-five grades lower than their highest level of educational attainment. Consequently, it is not unusual for someone with a high school diploma to be reading at a 7th to 9th grade reading level. Because of that gap, literacy experts recommend that materials written for the "general public" be at about a junior high reading level. In this study, a software analysis of readability determined grade levels from 11.92 to 14.11—much higher than the 7^{th} to 9^{th} grade level recommended. The results of this study confirm that online privacy policies have similar readability problems when compared to the Gramm-Leach-Bliley privacy statements required in the financial industry.

If an organization has a privacy policy but no one truly understands it, what is the point? Many policies continue to be confusing because privacy is inherently complex. The policy needs to clearly and accurately communicate the means that consumers have to access information contained about them. The goal of the privacy practices of any organization should be to instill trust that the organization will respect consumer privacy and personal information.

Privacy auditors say that many policies are contradictory. The participants in this study also expressed concern in contradictions that they found in the policies evaluated. The evidence discovered in this study verified that consumers had concerns that in a privacy policy, different positions could be stated within the same policy. For example, one statement could contradict statements made in other sections of the policy regarding the sharing of data. Organizations could state that they do not sell or rent customer data in one section of the policy notice; but later statements provided in the policy (on either the same or a different Web page), could state that the organization may pass data to unnamed third parties. As validated by the participants in this study, organizations that present contradicting statements damage consumer trust. Several evaluators in this study expressed a serious lack of trust in an organization based on what they felt were contradicting statements, which left them confused.

7. Benefits versus Concerns

This study further validated that our information age economy generates an enormous amount of data. The information revolution provides enormous benefits for consumers. However, many consumers fail to appreciate that today's average American enjoys access to credit and financial services, shopping choices, and educational resources that Americans from previous generations could never have imagined. Currently, we can check our credit card and bank balances over the phone or Internet 24 hours a day, we can order books, CDs, computers, clothes, or gifts online before we leave our home in the morning, or we can review our finances in a convenient consolidated statement at our convenience. Due to our credit reporting system involving personal financial data, instant credit is available to today's consumers. The system functions because, without the consumer's consent, very sensitive information about a person's credit history is shared with the credit reporting agencies. If consent were required, and consumers could decide—on a creditor-by-creditor basis—whether they wanted their personal information reported, the system would collapse. Credit histories are one of our most sensitive pieces of information—next to health and medical information. Many of the evaluators participating in this study expressed an appreciation for the value of

some information sharing that contributes to their quality of life. Most of them have enjoyed the convenience of online shopping.

However, despite the benefits of information sharing, concerns about privacy are genuine and legitimate among the participants in this study. Many participants were concerned by the extent to which their information is collected and used and were excited about having the opportunity to investigate how their information is being utilized. Some feel that they have lost control over their own information. Generally, consumers are concerned about the significant consequences that can result when their personal information is misused.

One risk identified in this study deals with economic injury. The fear of identity theft plagues the information age. Identity theft captures the fears that many consumers have about their privacy. It strikes randomly and it leaves financial injury difficult to rectify. Identity theft can range from unauthorized use of your credit card to someone creating a duplicate of you. Identity theft tarnishes your credit record and can result in the loss of credit, employment, and housing opportunities. Some victims can even find themselves facing criminal charges.

Another valid concern of consumers is the unwanted intrusions in their daily lives. As a result, the consumer receives unwanted solicitations for all types of products and services. Individually, the injury is relatively small, but taken together the harm can be great.

The concern and involvement is growing. Online privacy has become a hot topic for companies, government agencies, and watchdog groups. Although more Web sites are posting privacy policies, there continues to be concern regarding the quality of the privacy policy. In this study, it was found that the information that organizations learn from a customer assists the organization in personalizing and continually improving the customer's shopping experience. This study validated that while many customers appreciate the personalization made possible through available online technologies, some customers feel "tracked" by this same technology. An outcome of this discovery is the confirmation that privacy is a value that must be weighted against other values in our society.

8. Children's Privacy

Consumers tend to be especially concerned when they learn that their children are being asked for personal information on the Web. The potential for abuse extends beyond junk mail or marketing promotions that parents may consider inappropriate. Following is an example that strikes fear into the heart of any parent. According to the Newsbytes, Inc. (1996), a TV reporter successfully ordered 5,500 names and addresses of children from a marketing company called Metromail—using the name of "Richard Allen Davis," a convicted child murderer. The right information in the wrong hands is a tremendous cause for concern in the Information Age.

Both commercial sites evaluated in this study (Dell.com and Amazon.com), referenced a Children's Privacy Policy on their main privacy policy page. It is imperative to note in this study that separate privacy policies must exist for children less than 13 years of age.

There is no question that the privacy of children is important. According to the Federal Trade Commission (FTC), the Children's Online Privacy Protection Act (COPPA), which became effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online (FTC, 2001).

Unfortunately, due to the lack of education about this requirement, some evaluators participating in this research study were offended by strict regulations for children. One evaluator even commented that she would no longer shop at Amazon.com because she felt that her child was not welcome. Organizations need to improve in their commitment to consumer education. An informed consumer is more apt to be a better customer. Additionally, it has been discovered in this research study that consumers were not the only uninformed individuals. Many employees who are responsible for the administration of online data in organizations were unaware of COPPA, as well. Education and training will be vital as privacy concerns continue.

9. The Future of Information Privacy

The future of the online marketplace will be dependent, in part, on the future of information privacy. Privacy is one of the most critical concerns when assessing the opportunities and risks presented by Internet and information technology. The magnitude and economic importance of the information industry, as well as the depth of public concern, have made privacy a continuing political issue, which has been verified in this study. Although it would be difficult to predict the methods that will be used to resolve the privacy challenges, there are some trends and concepts that I believe will prove vital to the privacy debate:

1. If consumers want privacy, they will need to become better educated and more knowledgeable in security and technical issues, as well as marketing and legal issues.
2. Organizations doing business utilizing the Internet have strong business interests in fulfilling the privacy desires of consumers to win consumer trust.
3. Global pressures from the European Union will force a more unified international privacy agenda.
4. Frustrations with continuing privacy abuses may lead to regulations that do not take the realities of the dynamic nature of the Internet into account. These regulations could have unforeseen negative consequences due to the potential to stifle the Internet economy.
5. Although self-regulation efforts by businesses are widespread, privacy advocacy groups will continue to demand government regulation and continue to point fingers at Internet industry leaders who will serve as privacy scapegoats in the e-commerce marketplace.
6. Public perception of the risks of privacy violations will propel demands for regulation at the Federal level.
7. Online privacy policies will continue to change at any time, and without notice. Caveat Emptor! Let the Internet surfer beware.
8. Privacy policies commonly declare that they do not sell or rent customer data but in later statements provided in the policy or Web site, the policy states that the organization may pass information to unnamed third parties. Contradictions in statements will continue to destroy consumer trust.
9. A significant privacy threat will continue to be the use of enriched data or profiling. The merging of data from third parties will continue to be a concern for consumers.
10. Because of the electronic marketplace, organizations are developing privacy policies, which will flow into the non-virtual marketplace, as well.
11. If customers are to trust a Web site, they need to understand the privacy policy. Developing a privacy policy that incorporates very technical jargon in combination with legalese contributed by legal counsel will not achieve the goal of creating trust.
12. Only the surface has been touched. There is greater potential to utilize personalization in the electronic relationship with the consumer—by more fully understanding the consumer's profile and driving much more relevant content to the Web page. As a result, marketing to the customer based on the history of previous purchases and expressed interests will be more cost effective.
13. New technologies will continue to be developed to assist in maintaining data privacy for the Web user. Concurrently, new technologies will be utilized by organizations to offer even more extensive, personalized online experiences for consumers.
14. Privacy is not recognized as an absolute value in today's marketplace. Rather, it is one that will need to be balanced against other values.
15. There is not a "magic bullet" for solving privacy concerns on the Web. A combination of technology, policies, and education will be necessary.

10. Recommendations for Further Research

The privacy debate is a controversial and political issue that will not easily vanish. As new technology and the legal landscape change, additional issues will need to be addressed. Several critical areas have been selected as directions for future research. The results of further exploration into these areas have the potential to benefit consumers, as well as the e-commerce business environment.

11. Cyber-terrorism and Privacy

Following the September 11, 2001, terrorist attack on the World Trade Center, we need to examine how to balance our deeply-rooted commitment to civil liberties, such as privacy, with the fundamental need to protect society from the horror of terrorism. Further exploration into privacy issues in the context of preventing cyber-terrorism would be worthy of further academic research. Organizations have always faced the risk of hackers stealing sensitive data or launching virus and denial-of-service attacks. However, after The World Trade Center attack, the stakes are higher and may lead businesses to question the whole idea of Internet collaboration. As companies increase emphasis on security, will they take steps to collaborate more closely with partners, customers, and even competitors?

The same rewards that the Internet and advanced information technology provide to the general public and to business—speed, security, and global linkage—are assisting international terrorist groups coordinate their deadly and disruptive activities. The Internet and e-mail offer the perfect channels for these groups to communicate with each other, to distribute their messages, to raise money, and to launch cyber-attacks. Shall we forget about the protection of personal privacy of law-abiding citizens as we attempt to track terrorists through usage of the Internet and information technology?

Most online privacy policies contain provisions for sharing customer information with law enforcement agencies in the event of a criminal investigation or suspected illegal activity. However, are possible privacy violations occurring following the September 11, 2001, suicide hijackings that destroyed the World Trade Center? When is it appropriate to distribute complete databases to law enforcement without requiring a court order or a subpoena?

Organizations need to assure that their online privacy policies do not neglect the extensive investigations necessary following the terrorist attacks. Will this prompt some organizations to rewrite their published privacy statements and what effect will that have on consumer's uneasiness with data distribution? Further investigation into these concerns would be beneficial for society in general.

12. Identity Theft

One of the pressing concerns that consumers have regarding online privacy issues deals with the fear of identity theft. The risk of identity theft is a real threat whether the thief steals the information from an online Web site with a list of credit card numbers or from a consumer's mailbox. The findings of this study show that concerns exist that an increase in identity theft has occurred due to the growth of commerce on the Internet. To the degree that identity theft inhibits the Internet and e-commerce from reaching its maximum potential, we will all be affected negatively.

The fear of identity theft plagues the information age. Identity theft captures the fears that many consumers have about their privacy. The consequences are serious because it can leave financial injury, which can be difficult to resolve. Some victims of identity theft can even find themselves facing criminal charges. With such serious outcomes of identity theft, it stands to reason that consumers would have serious concerns regarding privacy of their personal information. Measures must be taken to combat identity theft because a proactive approach is much better than trying to rectify the damage of the crime. For the purposes of further research, the broader topic of how to combat online identity theft could be divided into three subject areas: victim assistance, prevention, and law enforcement.

13. Effectiveness of Privacy Protection Technologies

With the fear that loss of privacy has on consumers and the impact that this has on the economics of the information age, it can be expected that some companies will take advantage of this fearful consumer population. When companies deliberately market a product as one that enhances privacy or security, they are targeting consumers who not only care about these protections but also are willing to pay for them. Are the developers of these products truly delivering on the promise to ensure data privacy? Further research is always beneficial when it focuses on the effectiveness of any technological product in meeting goals and promises to consumers.

After many years, the Platform for Privacy Preferences ("P3P") is coming online. This cutting edge technology, one of many industry-driven initiatives, promises to give individuals much greater control over the collec-

tion of information, allowing them to specify their privacy preferences electronically and screen out sites that do not meet those preferences. This approach is believed to be much more manageable than today's site-by-site, notice-by-notice regime. As with any new technology, the implementation of this new technology should be monitored and its impact should be assessed.

14. Learning from the Gramm-Leach-Bliley Experience

Privacy notices were mailed to consumers in their bank statements, credit card statements, investment reports, mortgage statements, insurance mailings, and other financial statements during the summer of 2001. The federal Financial Services Modernization Act, also known as Gramm-Leach-Bliley (GLB), requires customers to be offered the choice to opt-out of their bank's sharing of personal information with third parties.

The recent experience with Gramm-Leach-Bliley privacy notices, sent to consumers in Summer 2001, brings concerns about whether we know enough to implement effectively broad-based legislation based on notices. Because of this law, reams of barely comprehensible privacy notices were distributed to consumers of financial services in the United States. Is it possible that the group reaping the most benefits from this law was the lawyers who wrote the privacy notices? Many believe this. Can organizations be more effective? A focus needs to be placed on how government and industry can make privacy notices more useful. We need to further research and examine our experience with Gramm-Leach-Bliley and learn from it. What did it accomplish? Did it benefit the customer? What would we do differently next time? We must use the experience as a foundation to ensure that any future privacy legislation accomplishes more than what has been described as creating a digital mattress tag. Compliance with Internet privacy legislation will have some costs, and consumers ultimately will pay the price. Although there are also benefits from online privacy legislation, we need much better data than we have about the cost/benefit tradeoff before we proceed.

15. Conclusion

The evidence uncovered in the collection of data in this study strongly supports the need for a fundamental need to educate individuals and organizations regarding the importance of finding a balance in the online privacy debate. Privacy is not recognized as an absolute value in today's marketplace—it is one that needs to be balanced against other values.

The study further suggests that, in at least one way, the electronic marketplace is no different from the business environment of years past. Survival of the fittest remains as the predictor of business success. The last issue that online retailers need to deal with at this time is additional negative media reports. In this new century, the big story in high tech has been the distressing burst of the "dot-com" bubble and the inevitable effects—layoffs, site closing, and the loss of available funding. Those "dot-com" businesses that are surviving in tough economic times are struggling with another challenge—the issue of the "ethics of data."

The problem is uncomplicated—the solution is not as simple. Organizations need to collect information that will assist in targeting promotions. On the other side, consumers want the convenience of secure e-commerce without worrying about having their identities stolen, being spammed, or having the collectors of their personal data knowing—and profiting from—information about them.

Some high-tech companies say increased privacy demands place an excessive burden on their businesses. However, critics from consumer rights groups and even some business advocates argue that the savvy online businesses will direct that resistance into a proactive approach. In other words, a privacy-friendly position could win over more potential customers than a hard line approach. By making their systems compliant with whatever privacy standards are set and taking advantage of some innovative new tracking and encryption technologies, organizations could eventually be capable of offering consumers the protection they want without losing sales. That could involve collecting the same data the organizations have always collected, but not distributing it to others without first getting permission or assuring customers that sites that inevitably will track their Web movements are held responsible for their practices.

This suggests that if people passively accept new data-gathering technologies, privacy will erode. The future of privacy will be determined by choices about how much privacy we as a society think is reasonable to de-

mand—not by the nature of the Internet. In the Information Age, people need to be willing to divulge some of their data to participate in daily life. The question is how to restrict abuse of the data collection and ownership. Fair Information Practice Principles provide the foundation to move forward in this debate. It has become clear that in this era, the opposing sides will find common ground only if each agrees to give up part of something they once considered their divine right. 🕮

References

1. Amazon.com (2000). "Amazon.com Privacy Notice". *Amazon.com*. Retrieved November 15, 2000, from *http://www.amazon.com/exec/obidos/tg/browse/-/468496/104-9914041-4611941*
2. Anderson, D. L. (2000). *Management information systems: Using cases within an industry context to solve business problems with information technology*. Upper Saddle River, NJ: Prentice Hall.
3. Clayton, G. (2000, July 17). "Privacy evaluation: Dell". *InformationWeek*. Retrieved July 26, 2000, from *http://www.informationweek.com/privacy.dell.htm*
4. Dell Computer Corporation (2001). "Online Privacy Practices. Dell Computer Corporation". Retrieved November 15, 2000, from *http://www.dell.com/us/en/gen/misc/policy_000_policy.htm*
5. Disabatino, J. (2001, November 9). "Security hole in IE reveals data in cookies". *ComputerWorld*. Retrieved November 10, 2001, from *http://www.computerworld.com/storyba/0,4125,NAV47_STO65588,00.html*
6. Electronic Privacy Information Center (1999, December). "Surfer Beware III: Privacy Policies without Privacy Protection". Retrieved October 15, 2001, from *http://www.epic.org/reports/surfer-beware3.html*
7. FTC (1999, November). "How to Comply With The Children's Online Privacy Protection Rule Children's Privacy". Retrieved October 15, 2001, from *http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm*
8. FTC (2000, May 15). "Final Report of the FTC Advisory Committee on Online Access and Security". Retrieved May 15, 2000, from *http://www.ftc.gov/acoas/papers/finalreport.htm#III*
9. FTC (2000, May 25). "Privacy Online: Fair Information Practices in the Electronic Marketplace". Retrieved September 2, 2000 from *http://www.ftc.gov/os/2000/05/testimonyprivacy.htm*
10. Hawkins, D. (2000, December 4). "Guarding your online privacy". *Online U.S. News*. Retrieved August 1, 2001, from *http://www.usnews.com/usnews/issue/001204/nycu/moneyb.botw.htm*
11. Hochhauser, M. (2000, November). "Why I stopped shopping at Amazon.com: A reading expert sounds off". Retrieved July 18, 2001, from *http://www.privacyrights.org/ar/amazon.htm*
12. Hochhauser, M. (2001, November). "Lost in the fine print: Readability of financial privacy". Retrieved November 18, 2001, from *http://www.privacyrights.org/ar/GLB-Reading.htm*
13. Kincaid, J. (2001, March). "Devise a customer privacy policy…and stick to it". *Target Marketing*, 24(3) 32.
14. Kontzer, T. (2001, November 16). "Dell's third-quarter rebound". *Information Week*. Retrieved November 16, 2001, from *http://www.informationweek.com*
15. Linn, A. (2001, March 12). "Amazon explores new profit areas". *The Herald-Dispatch*. Retrieved August 1, 2001, from *http://www.hdonline.com/2001/March/12/Lnlist1.htm*
16. McCullah, D. (2001, June 2). "The case against privacy". *Wired Online*. Retrieved July 2, 2001, from *http://www.wired.com/news/privacy/0,1848,44255,00.html*
17. McNealy, S. (2001, May 29). "The case against absolute privacy". *The Washington Post Online*. Retrieved July 2, 2001, from *http://washingtonpost.com/wp-dyn/articles/A89273-2001May28.html*
18. Naini, M. J., & Gabrieli, D. (1999, June 11). "Re: Children's Online Privacy Protection Rule—Comment, P994505" (Letter addressed to the FTC.) Retrieved August 1, 2001, from *http://www.ftc.gov/privacy/comments/amazoncom.htm*
19. Newsbytes (1996, May 23). "Feinstein bill to keep info on children private". *Newsbytes Inc.* Retrieved November 17, 2001, from *http://www.epic.org/privacy/kids/newsbytes.txt*
20. Online Privacy Alliance (2001). "Our Privacy Policy". *Online Privacy Alliance*. Retrieved November 15, 2000, from *http://www.privacyalliance.org/about/privacypolicy.shtml*
21. Rodger, W. (2000, June 7). "Privacy isn't public knowledge: Online policies spread confusion with legal jargon". *USA Today*. Retrieved August 1, 2001, from *http://www.usatoday.com/life/cyber/tech/cth818.htm*
22. Rose, F. (2001, October 4). "Beales explains new FTC pro-privacy plan: Increased resources, enforcement efforts at heart of plan". *The Progress & Freedom Foundation*. Retrieved November 3, 2001, from *http://www.pff.org/pr/pr100401Beales.htm*
23. Rosen, A. M. (2000, December 4). "Internationally recognized Internet privacy expert has advice for on-

line shoppers this holiday season". *OPA News*. Retrieved September 18, 2001, from *http://www.privacyalliance.org/news/01052001.shtml*

24. Soto, M. (2001, May 26). "FTC clears Amazon privacy policy". *Seattle Times*. Retrieved October 15, 2001, from *http://seattletimes.nwsource.com/html/businesstechnology/134299495_amazon260.html*
25. Sprenger P. (1999, January 26). "Sun on privacy: 'Get over it.'" *Wired News*. Retrieved June 25, 2001, from *http://www.wired.com/news/politics/0,1283,17538,00.html*
26. Sullivan, A. (2001, May 25). "FTC: Amazon privacy practices did not break law". *WashingtonPost.com*. Retrieved November 1, 2001, from *http://www.washtech.com/news/regulation/10044-1.html*
27. The Software and Information Industry Association (2000, May 25). "Senate Commerce Committee holds hearing on privacy (May 16 testimony by Varney)". Retrieved October 15, 2001, from *http://www.siia.net/sharedcontent/govt/issues/privacy/5-25-00.html*
28. University at Albany (2000, Spring). "Regulating Cyberspace". Retrieved November 3, 2001, from *http://www.albany.edu/pr/albanymagspring2000/cyberspace.htm*

Notes