TURUN KAUPPAKORKEAKOULUN Jjulkaisuja

PUBLICATIONS OF THE TURKU SCHOOL
OF ECONOMICS AND BUSINESS ADMINISTRATION

Olli Järvinen

PRIVACY MANAGEMENT OF E-HEALTH
Content Analysis of 39 U.S. Health Providers' Privacy Policies

Sarja / Series A-3:2005

ISBN 951-564-297-3 (nid.) 951-564-298-1 (PDF)
ISSN 0357-4652 (nid.) 1459-4870 (PDF)
UDK 004.5
004.7
681.324
614 (73)
342.72/.73 (73)
65.012.45
17

Esa Print Tampere, Tampere 2005

ACKNOWLEDGEMENTS

This work has been supported both intellectually and financially by a multitude of people and institutions. I take this opportunity to express my gratitude to all those who have made it possible for me to begin and complete my doctoral thesis.

I had the great pleasure of working as a Fulbright ASLA researcher, from August 2001 to June 2002, at the Department of Business Management of the North Carolina State University, Raleigh, USA. Many insightful ideas of this thesis result from that time. First of all, I owe my deepest gratitude to the researchers at North Carolina State University and Georgia Institute of Technology, Atlanta, especially Professors Gary Dickson, Annie Antón, Julie Earp, and Colin Potts. They and their colleagues have provided me with a forum to exchange research ideas. Special acknowledgements to you Gary, your hospitality during our visit at North Carolina State University was something which I and my family never forget.

I sincerely thank the official examiners of this study, Professor Inger Eriksson and Docent Mikko Korpela, for their time and excellent comments that helped me a lot. It has been a great privilege to have two experienced reviewers from the IT-ethics research area. Their interests in my research and recommendations have been of critical importance to me. I was very pleased to read the first examination reports which finally assured me that the study was important and interesting. Professor Inger Eriksson has reviewed the manuscript with a precision and thoroughness that very few people are capable of. I specially want to thank Docent Mikko Korpela, who accepted the invitation to act as an esteemed opponent of my thesis.

I have the privilege to have many good advisors around me. Professor Markku Nurminen's enthusiastic grip especially at the beginning of my research career was essential. Special thanks are also reserved for my supervisor, Professor Hannu Salmela for his patience with the author's 'almost ready' project. Thank you Hannu – your help made it possible to complete my doctoral thesis effectively. I would express my gratitude to all colleagues at the Turku School of Economic and Business Administration for their invaluable comments on the manuscripts of the thesis. Dozens of anonymous reviewers of my earlier works have also contributed through constructive comments. There are also plenty of other persons who deserve sincere acknowledgement for their comments on my papers, fruitful discussions, and the like. Senior Lecturer Satu-Päivi Kantola merits thanks for guiding me

through the statistical puzzles. Thanks to Mester Translation House Ltd for checking and revising the language of the thesis.

I would like to thank Rector Tapio Reponen and the Turku School of Economics Association for their support in the dissertation process. I thank the researchers and administrative staff of Information System Science at the Turku School of Economics and Business Administration for creating a positive and helpful working environment. Special thanks go to Secretary Birgit Haanmäki for taking care of many practical things. The libraries of Turku School of Economics and Business Administration and Turku University deserve thanks for excellent service.

Personal support is extremely valuable, but so is financial. I would like to express my gratitude for the financial support I have received. This study was funded by research grants from the Academy of Finland, the Foundation for Economic Education and the Fulbright Center. In addition, the Emil Aaltonen Foundation, the Ella and Georg Ehrnrooth Foundation, the Yrjö Jahnsson Foundation, Instrumentariumin Tiedesäätiö, the Finnish Cultural Foundation, and Turun Kauppaseuran säätiö are acknowledged for their support. This support enabled fluent progress of the project, whilst also giving me an indication that somebody else is also interested in my work and that it might be important.

My biggest thanks go to my family. This has been a very hard time for me, but it must have been even harder for you. I want to give my warmest and personal thanks to my wife Riitta, my son Erkka and my mom Helena. I especially thank them for all their relentless support and patience during these past years. This research would never have been completed on time if not for their encouragement and sincere support.

Turku, June, 2005

Olli Järvinen

TABLE OF CONTENTS

FIGURES, TABLES, AND EXAMPLES:

Figures:

Tables and Examples:

1 INTRODUCTION

> *"For the most part the need for privacy is like good art, you know it when you see it. But sometimes our intuitions can be misleading."*
> *(Moor, 1997, p. 28).*

1.1 Background

In a computerized society information moves fast and globally. Information and communication technology will play an increasing and essential strategic role in the present society of networks. Today's global economy offers Internet users unprecedented access to a wide range of goods and services. The Internet offers a straightforward means to interact with other business institutions, services and individuals at a very low cost. Several online organizations are involved in collecting, sharing and using customer information, and these processes need to be as privacy protective and trustworthy as possible. In a computerized culture the concern for privacy is legitimate and well grounded. Privacy can be seen as one of our expressions of the core value of security. Individuals and societies that are not secure do not flourish and do not exist for long. The topic is justified because more research is needed to address how we as a society use, value, and protect citizens' personal information.

The Internet has opened up many new ways for people to communicate, and the result for these people is more spending, more time using, more data-rich applications, and more replication and caching of data. As customers gain experience, many Net surfers seem less dazzled by the Internet. The Internet has become a mainstream information tool. Its popularity and dependability have raised expectations about the information and services available online. As a result, more people use the Web to get news, financial information, Government information and product information. The status of the Internet is shifting from being a dazzling new thing to being a purposeful tool that people use to help them with some of life's important tasks. As Internet users gain experience online, they increasingly turn to the Internet to perform work-related tasks, to make purchases and do other financial transactions, to write emails with weighty and urgent content, and to seek information that is important to their everyday life (Horrigan and Rainie, 2002, p. 17).

The number of people who use the Internet to find health care information has been on the rise. People increasingly use the Internet to obtain health information (Cline and Haynes, 2001; Fox, 2001; Landro, 2000; Spooner and Rainie, 2001a; Spooner and Rainie, 2001b). The Pew Internet & American Life Project[1] first began tracking Internet behavior relating to health in March 2000. For example, it was reported that 52 million American adults relied on the Internet to make critical health decisions at that time. Since then the numbers have been steadily rising. Based on a national survey in March 2002, an estimated 73 million Americans have used the Internet for health information (Rainie, 2002). By March 2003, 77 million American adults said they go online to look for health or medical information (Fox and Fallows, 2003). Mark Bard of the Manhattan Research Group (2002) has coined a term that captures the "*searching for someone else*" phenomenon. When counting those who actively use online health resources, researchers should calculate a much larger "*zone of influence*" made up of friends, family members, co-workers, and neighbors who also benefit from customers' searches. Health care is often a highly social pursuit, not just a solitary activity. It is essential to reflect this reality when researching, serving, or creating policies for a customer population (Fox and Fallows, 2003, p. 21).

The largest increments of growth in health care activities came among Internet "veterans"[2]. While the Internet population has stabilized at about 60% of Americans over the last two years, the number of veteran Internet users has grown substantially (Lenhart, 2003). It is known that the longer someone has been online, the more inclined they are to feel more confident about their ability to find valuable information on the Web and report using that information to make decisions in their lives (Horrigan and Rainie, 2002). Customers[3] use the Internet to investigate many health-related topics commonly encountered by primary care providers (Diaz, Griffith, Ng, Reinert, Friedmann, and Moulton, 2002). Customers use the Internet to research prescription drugs, explore new ways to control their weight, and prepare for doctor's appointments, among other activities (Fox and Rainie, 2002).

---

1 The Pew Internet & American Life Project creates and funds original, academic-quality research that explores the impact of the Internet on children, families, communities, the workplace, schools, health care, and civic and political life. The project is an independent, non-partisan organization that aims to be an authoritative source of timely information on the Internet's growth and its impact on society. The project's Web site: www.pewinternet.org

2 "Veteran" Internet user – someone who has been online for three or more years.

3 Internet users who search for online information on health topics, whether they are acting as consumers, caregivers, or e-patients. For shorthand purposes, they are called "customers" throughout this dissertation.

However, health Web sites please customers more than they please health care professionals. The results of the California HealthCare Foundation/RAND study demonstrated those concerns. Only half of the topics that the expert panels thought were important for consumers were covered more than minimally. Some experts warn about a danger – the best information is not even on the Internet. The study found substantial gaps in the availability of key information relating to breast cancer, depression, obesity, and childhood asthma available thorough Web sites. (Berland, 2001). Another study echoed RAND's cautionary tone after comparing the 25 most popular health Web sites' adherences to quality codes, peer review, and external advisory boards (Eng, 2001). Additionally, the American Medical Association[4] (AMA) has taken the position that online health information is never a substitute for a physician's experience and training, suggesting that people should trust their physician, not a chat room (AMA, 2001).

Widespread skepticism among medical providers has not slowed the remarkable growth in the number of people seeking medical information online. More people research health information online on an average day than visit health professionals. About 6 million Americans go online for medical advice on a typical day, whereas the American Medical Association estimates that there are an average of 2.75 million ambulatory care visits to hospital outpatient and emergency departments per day and an average of 2.27 million physician office visits per day (Fox and Rainie, 2002). Additionally, over 45 million Americans say the Internet has improved the way they take care of their health either "*a lot*" or "*some*". Whether the health information is needed for personal reasons or for a loved one, millions of health-related Web pages are viewed by millions of consumers (Fox and Rainie, 2002).

Sometimes the information found is just what was needed. Other searches end in frustration or retrieval of inaccurate, even dangerous, information. But it could be the case that consumers are so pleased with the convenience of getting health information online that they are prepared to forgive any shortcomings of online medical advice. In an August 2000 survey, over 90 percent of customers said it is important that they can get health information when it is convenient for them. (Fox and Rainie, 2002).

Wider use of the Internet has also been growing rapidly during the past few years. The Internet has created a "*universal*" technology platform upon which

[4] The Medical Library Association is an educational organization of professionals providing quality information for improved health. Founded in 1898, MLA represents more than 1,100 institutions and 3,800 individual members in the health sciences information field.

all sorts of new products, services, strategies, and organizations can be built. The Internet enables new means to provide services for knowledge-intensive industries such as insurance, banking and health care. The new applications appear to challenge the traditional ways of how services are delivered and consumed. In this thesis, electronic commerce (e-commerce and e-health) is understood as the process of buying and selling (health) goods and (health) services electronically with computerized business transactions using the Internet. It encompasses activities supporting those market transactions, such as information sharing, advertising, marketing, customer support, delivery, and payment.

By replacing manual and paper-based practices with electronic alternatives, and by using information flows in new and dynamic ways, electronic commerce can accelerate ordering, delivery, and payment for goods and services while reducing companies' operating and inventory costs. Even with so many dot-com companies going out of business, online purchasing by consumers has followed a steadily upward path. The year 2001 was significant in the history of electronic commerce. Despite the economic slowdown and the present vulnerability of dot-com ventures, online sales revenues worldwide are expected to reach $550 billion, a 92 percent increase from 2000 (e-marketer, 2001). It is expected that by the year 2004, global electronic commerce will generate $3.2 trillion in revenues (e-marketer, 2001). For example, in March 2000, 40 million Americans had purchased a product online. That number grew to 72 million by the beginning of October 2002. This growth has occurred at a time when the United States has suffered a mild recession and subsequent tepid economic growth, and as consumer confidence has sagged. The main reason for the growth in the population of e-consumers is increasing comfort with online transactions for Internet users. Consumers' comfort with the online world breeds growing confidence in electronic commerce, even in the face of general declines in consumer confidence. This explains in growth in consumer buying online. (Horrigan and Rainie, 2002, p. 14).

A major benefit of interactive Web-based content is that it makes the provision of customer service less expensive (Honeycutt, Flaherty and Benassi, 1998) and interactive Web-based applications facilitate the customization of service and product offerings for individual accounts, offering companies infinite opportunities to learn more about each customer's specific requirements and business operations (Zemke and Connellan, 2001). Electronic commerce involves "*the use of computer networks to improve organizational performance*" (Watson, Berthon, Pitt and Zinkhan, 2000, p. 1).

The Internet provides companies with opportunities to enhance business offerings in a practical manner (Fontanella, 2000). It can help companies increase profitability, reach new markets, improve customer service, distribute products faster, and communicate more effectively with supply chain partners (Kleindl, 2001; Watson, Berthon, Pitt and Zinkhan, 2000). The Internet enables globalization of business relations (Cronin, 1995). The Internet has an important impact on the relationships between firms and external entities, and even on the organization of business processes inside a firm. Organizations can create intranets, which are internal networks based on the Internet, to reduce network costs and overcome connectivity problems. Thus, the Internet increases the accessibility, storage, and distribution of information and knowledge for organizations, which is important because "*there is usually potential for improving knowledge capabilities, both within and between units of an organization. But external or inter-organizational possibilities may be at least as attractive and ultimately more important. These include, for example, mutual sharing of knowledge with partners, allies, intermediaries, suppliers, and customers*" (Earl and Scott, 1999, p. 30). This is why businesses are rebuilding some of their key business processes based on the Internet technology.

If the Internet has opened up many exciting possibilities for the use of information systems, Harriet Pearson[5] (2003) suggests that there is much more to come. She thinks that the Internet revolution is less than 5 percent complete. The amount of content and number of applications, users and devices is increasing. She suggests that the total amount of data connected to the Internet will progress as follows:

- 2001 – one petabyte (10^{15} bytes).
- 2006 – one exabyte (10^{18} bytes).
- 2010 – one zettabyte (10^{21} bytes).

Along with providing many new benefits and opportunities, the Internet has also created a new set of management challenges. Most major advances in technology also entail unintended consequences; modern technology has increased the potential for misuse (Baumer, Earp and Payton, 2000). "*Corporations and organizations are struggling to handle an exponential increase in the number of on-line transactions, to protect the privacy and security of proprietary and personal data, and to deal with the growing complexity of IT systems*" (Pearson , 2003).

[5] Vice President and Chief Privacy Officer of IBM Corporation.

Most health Web sites are pitched publicly as tools that give consumers greater control over their lives and their health care. However, many Web sites require users to provide a great deal of sensitive health information, and they may also collect information on users without the users' knowledge or consent. Health care providers maintain and share a vast amount of sensitive patient information for a variety of reasons. Such records are kept and shared for diagnosis and treatment of the patient, payment of health care services rendered, public health reporting, research, and even for marketing and use by the media (Choy, Hudson, Pritts and Goldman, 2001, p. 3). When transactions are stored and exchanged using electronic services, personally identifiable information such as electric receipt and purchase orders become more widely accessible and potentially vulnerable (Udo, 2001).

Because the Internet revolution has the potential to have major effects on how we lead our lives, the paramount issue of how we should control the Internet services and the flow of information needs to be constantly addressed in order to shape Internet technology to serve us to our mutual benefit. It is imperative that we create principles, policies, and practices of privacy that allow citizens to rationally plan their actions without threat of privacy invasion. When formulating privacy practices and policies, companies should try to minimize excess harm and risk of customers' personal information. This is important because e-business will only grow if organizations and societies address privacy concerns.

Customers are very anxious to have their privacy protected. Since the inception of commercial activity on the Internet, privacy has been perceived by some to be a significant barrier to the emergence of a consumer mass market on the Internet. Additionally, from the customers' perspective, concern about the Internet's lack of security and unreliable technology have significantly impacted user acceptance of electronic commerce since its inception (DeCovny, 1998; Sterrett and Shah, 1998; (Watson, Berthon, Pitt and Zinkhan, 2000). The vulnerability of the Internet is huge because there is no central authority or management, and no one to install the technology or establish network-wide security and privacy policies.

> *"I would argue that from the start, the world-wide-web was a transparent rather than a sheltered environment, more like going from shop to shop in a large mall than, say, writing in one's diary in the privacy of one's home. Given the lack of any clear social norms or laws that control access to Internet wanderings, it is therefore unreasonable to expect privacy in this domain."*
> *McArthur (2001, p. 126).*

Privacy has emerged as a central policy concern about the Internet as more people go online every day. Not surprisingly, a great many people are fretful about the things that could happen online and the way in which data about them might be gathered and used. A strong sense of distrust shadows many Internet users' view of the online world, and the uneasiness has grown in the past two years. An overwhelming majority of Internet users are concerned about businesses or people they don't know getting personal information about themselves or their families (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 12). Many Web sites do not have adequate security in place to protect consumer information (Fox and Fallows, 2003, p. 29), for example, in recent years there have been breaches of privacy and security at the Web sites of major academic institutions (Choy, Hudson, Pritts and Goldman, 2001, p. 5). As a result of privacy and security failures, a 2002 survey[6] in the U.S. revealed that almost 80 percent of Internet users believed developers are creating Web-based applications so quickly that little planning goes into security and privacy measures. Customers are afraid of Web sites selling or giving away information about them, about insurance companies learning what they have done online and making coverage decisions based on that, and about their employers learning what they have done (Fox and Rainie, 2000).

The following provides some health business examples that illustrate how the customers´ vulnerability has been breached.

Prozac.com, a Web site owned by the drug company Eli Lilly and Co., provides information about depression. Until recently, individuals could sign up for an Internet service that would send them email reminders about taking their Prozac medication. The email messages were addressed to individuals. Later the company sent the customers an email informing them that the service was being canceled. The message, however, was addressed to all of the participants. This email contained all the email addresses of the customers currently using this service. So Eli Lilly and Co. inadvertently revealed 600 customers email addresses (Wilson, 2001; O'Harrow, 2001). When Eli Lilly unintentionally released the email addresses of customers on Prozac, the privacy practices of health-related Internet services received much attention in the press, but this is not the only case.

Global Health Trax sells over-the-counter health and nutrition supplements online. It inadvertently revealed customer names, the home phone numbers, and bank account and credit card information of thousands of its customers on its Web site (Sullivan, 2000). Additionally, Life insurance broker SelectQuote

[6] http://www.theprivacyplace.org

Insurance Services exposed some of its customers' personal information, including health information, on its Web site. Information that was submitted by customers to obtain life insurance quotes was not "*cleared*", and thus remained on the site and could be viewed by subsequent customers (Bunker, 2000).

In summary, the threat that existed over 100 hundred years ago is very topical. Warren and Brandeis (1890) felt that numerous mechanical devices make good on the prediction that "*what is whispered in the closet shall be proclaimed from the house-tops*." The presented cases are surely one reason that less than one in ten customers have set up a personal profile at a favorite health Web site or customized a health Web site so they receive only the information they are most interested in. Only about one-fifth of all customers have ever signed up for an electronic newsletter that emails the latest health news or medical updates (Fox and Rainie, 2002). However, a 2002 Harris Interactive poll found that nine in ten Internet users would like to email their doctor's offices – and over one third of them would be willing to pay for the service (Harris, 2002). As further evidence that email gaining a foothold, a 2001 Harris Interactive poll found that many doctors were initially skeptical about the benefits of online tools, but were pushed by patients to start using email and now say it has increased patient satisfaction (Harris, 2001).

Online customers have great concerns about breaches of privacy, while at the same time they do or they want to do a striking number of intimate and trusting things on the Internet. On some major points, though, there is a powerful consistency. The first point is that Internet users overwhelmingly want the presumption of privacy when they go online. The second point is that a great many Internet users do not know the basics of how their online activities are observed and they do not use the available tools to protect themselves (Fox, Rainie, Horrigan, Lenhart, Spooner and Carter, 2000, p. 2). Uslaner (2000, p. 18) suggests that many people see the Internet as more threatening than welcoming. "*There is a reservoir of suspicion that technologies beyond our control, often beyond our comprehension, are intruding on our personal lives, with less than benign intensions. This makes sense when we realize that mistrust reflects a pessimistic world view and a feeling that things are beyond our control*."

The sensitive nature of health care services suggests that there should be increasing interest in designing secure and privacy protected Internet services. It is probably not possible to eliminate all threats and vulnerabilities, but the risk of privacy invasion can be decreased to a level which is bearable. In addition, Keen (1997, p. 80) states that the most significant long-term barrier

for realizing the potential of Internet marketing to consumers will be the lack of consumer trust, both in the merchant's honesty and in the merchant's competence to fill Internet orders. This view is consistent with exchange theory (Thibaut and Kelley, 1959). According to exchange theory, individuals form associations on the basis of trust, and try to avoid exchange relationships that are likely to bring more pain than pleasure. Web site customers primarily want to know what the company offers, what it can do for them, and how and where they can obtain its product and services (Gallant, 1997; Zemke and Conellan, 2001). Web site design is also critical, because Internet users are in control of which sites they go to (Zemke and Connellan, 2001) and are probably less inclined to revisit Web sites that are not trustworthy.

In the Internet age, during a period when Internet services are growing rapidly and consequences are difficult to predict, it is more important than ever to be as clear as possible regarding how privacy should be understood and how it is justified. Privacy is becoming a standard issue for Internet ethics, because the widespread use of Internet services and the complexity of Internet infrastructure is a combination that makes solitude and privacy more essential to the individual. It is important to determine how privacy is applied and how it should be guarded widely, because consumer privacy concerns can pose a serious impediment to expanded growth of electronic commerce and Internet usage in the future. Even the most convenient Internet services may function ineffectively (Belanger, Hiller, and Smith, 2002; Cranor, Reagle, and Ackerman, 1999; Elofson, 2001; Udo, 2001). The major uncertainties and high levels of risk derived from the unknown nature of new information goods and services, transactions partners (or third parties, if one prefers to employ the standard Internet vocabulary), companies and economic activities suggest a high demand for development of trust-enhancing products and methods.

When new technologies are adopted, an organization's security policy and privacy policy must be revisited and often revised to respond to policy conflicts introduced by these new technologies. It is important to think of privacy in terms of customers' interest but also companies' interest. The thesis conception encourages informed consent as much as possible and fosters the development of practical, fine grained, and sensitive policies for protecting privacy when it is not. From the perspective of system design, customers need more easily understandably tools to gain control over organizations' privacy policies and practices.

Owing to the nature of the Web technology, the focus should be very global; the differences in cultures and languages, as well as licensing and liability regulations may affect the interaction between organizations and

customers, even though the business target itself is basically the same in every country. The success of firms in the future depends on their ability to operate globally. Organizations that cope best and trustfully with the uncertain conditions of global issues will be in the best position to gain business advantages on the Internet.

This explorative study is intended to help consumers and policy makers understand how privacy policies are expressed on health care Web sites. This thesis comments on what changes will be required for those Web sites to express their privacy policies more clearly.

1.2 Previous Studies

Issues concerning users' privacy protection on the Internet have been studied and especially discussed largely for some time. However, despite the interest in the topic, privacy issues of Internet privacy policies continue to be overlooked in the research literature. Several researchers have provided various approaches to creating sufficient data protection for consumers. Much emphasis is placed on data protection and confidentiality issues to prevent unauthorized use. Many of these approaches outline technical measures for providing better security, which in turn provide a higher potential for data privacy. Techniques such as encryption, secure transmissions, firewalls, password identifications, access control and many other technologies have been used (Memon and Wong, 1999; Schneier, 1996; Peterson, Balasubramanian and Bronneberg, 1997). Reducing the threats to sensitive data is also the focus of several studies addressing technical methods to provide better security for data privacy (Brannigan and Beir, 1995).

Some proposals and suggestion for how to deal with privacy issues involving information technology fall into one of two types or categories: proposals that are technology-based and those that are legislation-based (Tavani, 1999b, p. 271). Informational privacy issues are not only a matter of legal and technical issues and their mutual interaction. Business practices of the Internet call attention to an evolutionary approach for privacy policy development. Organizational routines and norms direct employees' actions, resulting in cumulative privacy policy utilization to support organizational goals, but by doing so they may also constitute a privacy threat to customers.

Some researchers (Smith, Milberg and Burke, 1996) have understood the need for validated instruments for measuring individuals' concerns about organizational practices. They have developed tools to identify and measure

the principal dimensions of privacy concerns. Their idea is that because employees of any organization are ultimately in control of sensitive customer information, it is important to understand employee attitudes, as well as consumer attitudes, toward privacy. Understanding the attitudes of employees, who have regular access to personal information, will assist the field in developing better methods for privacy protection. The literature also contains many studies pertaining to the general notion of privacy practices, for example, Dick Mason's PAPA-model[7] studies people's vulnerability (Mason, 1986), and Thomas C. Rindfleish (1997) prescribes privacy, confidentiality and security as the three primary concepts when considering data protection in health care organizations.

- Privacy: A person's right and desires to control the disclosure of his and her personal information.
- Confidentiality: The controlled release of personal information to an authorized information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.
- Security: Policies, procedures, and safeguards used to help control access to the contents of information systems (particularly databases) while maintaining the integrity and availability of the data.

Though many studies have examined the information available on the Internet, both in terms of customer's experiences and the quality of the information, little work has been done to evaluate the privacy practices of the Internet for health-related activities. All these previous studies and models are vital for effective data protection, but they are not wide enough or they lack a much-needed mechanism to evaluate the privacy element in more detail in the health care segment. For example, there is no agreement on how we should conduct the revision and evaluation of privacy practices and policies and which kind of factors ought to be taken into account.

A growing body of government researchers, market research organizations, and scholars has begun to focus on e-health, telemedicine, e-government and electronic commerce areas (Horrigan and Rainie, 2002, p. 5), and with the steady growth of Internet penetration, and the sometimes-fevered focus on the Internet's transformative potential, customers have begun to expect a lot from the Internet. This revolution in health care information has great potential to affect how customers' privacy is understood, but relatively few have studied

[7] PAPA means Property, Accuracy, Privacy and Accessibility of Information.

expressed online privacy policies[8] in the health care business segment. Previously, privacy policies have been evaluated in a rather ad hoc and inconsistent manner, but there is one exception. A study by Goldman, Hudson, Smith (2000) focused on the policies and practices of 21 health-related Web sites. The Web sites were selected to represent a mix of the most trafficked consumer health sites in the following groups: Web sites where consumer desire for anonymity might be more precious, Web sites where pharmaceuticals and health products may be researched and purchased, general search engines or portals that get a high degree of Internet traffic, and Web sites that target a specific demographic. They reviewed the privacy policies of each Web site and investigated whether their actual practices reflected their stated policies. Their method for the investigation was to review the stated privacy policies against a set of "*fair information practice principles*"[9] and to behave like a typical consumer on each Web site in order to observe and capture what happened to the data that was submitted. The major findings of their research are as follows:

- Visitors to health Web sites are not anonymous, even if they think they are.
- Health Web sites recognize consumers' concern about the privacy of their personal health information and have made efforts to establish privacy policies; however, the policies fall short of truly safeguarding consumers.
- There is inconsistency between the privacy policies and the actual practices of health Web sites.
- Consumers are using health Web sites to better manage their health, but their personal health information may not be adequately protected.
- Health Web sites with privacy policies that disclaim liability for the actions of third parties on the site negate those very policies.

Following the release of their report, several members of Congress requested that the Federal Trade Commission immediately initiate an

---

[8] The Federal Trade Commission (FTC) states that a privacy policy is a comprehensive description of an organization's information practices. It is located in one place on a Web site, and may be reached by clicking on an icon or hyperlink (FTC, 1998). More specifically, privacy policies inform consumers about how organizations collect and use their customer information and theoretically serve as a basis for consumer browsing and transaction decisions. Internet privacy policies are critical due to the increase in information collection for various business functions, as evidenced by the increased attention received by companies whose privacy practices come into question (e.g. FTC, 2000).

[9] These principles are presented in Section 2.3.2. See also The Code of Fair Information Practices, U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, viii, http://www.epic.org/privacy/consumer/code_fair-info.html, 1973.

investigation into whether certain health Web sites may be engaged in "*unfair or deceptive acts or practices*." (Pitofsky, 2000a; Pitofsky, 2000b). A subsequent Federal Trade Commission (FTC, 2000) investigation of several of these health Web sites found that the sites made changes to their policies in response to the findings of the report. Additionally, the study of Progress and Freedom Foundation (PFF) shows that commercial Web site privacy practices and policies are improving in two major ways: they are claiming they are collecting less information from consumers, and Web sites policies are increasingly reflecting fair information practices (Adkinson, Eisenach, and Lenard, 2002).

1.3 Aim of the Research

This thesis studies the privacy policies of health care Web sites to obtain more practical and useful knowledge of privacy practices in electronic commerce. The author argues that the older studies do not provide sufficient concept to answer questions such as: how to balance customers' interest in privacy with the benefits of having so much more data? And how would it be possible to balance the rights of customers to privacy against the desire of companies to use this technology to improve their marketing and to better target their products at the interests of customers?

Growing online experience results in greater skill at doing things online. Notwithstanding the dot-com shakeout, the passage of time has meant more useful content becoming available on the Web. The upshot is more health-related applications online and more experienced customers with greater ability to separate the wheat from the chaff. The result is high expectations about what is online. Our challenge is to take full advantage of the Internet without allowing the Internet companies to take complete advantage of us and, therefore, thoughtful analyses of newer privacy situations in which the Internet has an impact are needed. This explorative study is justified because more knowledge is needed to address and assess how organizations use, value, and protect customers' personal information on the Internet. It is possible that the potential of new Internet services might be partially used, and changing existing practices to reflect more privacy respectful actions might result in new, more acceptable services.

This study seeks to increase the understanding of privacy policy as a significant trust indicator for fair business practices. The objective of this study is to develop an instrument to assess the content and communication of

privacy policy. The study identifies how privacy policy statements interact to produce and sustain an online presentation of the company and produce a convincing performance.

This study is one of the first to address the relationship between consumer and business interests when focusing the Web sites privacy policies and, thus, this study is explorative by nature. The main research questions that guide this study are:

- What are the requirements for a good privacy policy of a Web site?
- What communication practices of privacy matters are found in health care Web sites?
- What are the typical contents of a health care Web site privacy policy?
- How to assess the content and communication of privacy policy?

To answer these questions, a content analysis of 39 expressed online health care privacy policies was conducted. In this dissertation, the role of the researcher should be seen as a rationalistic knowledge builder inquiring about privacy practices from the perspective of an online customer and focusing on a more communicable and usable understanding of privacy practices. This explorative study is intended to help customers, software engineers, and privacy managers understand how privacy policy statements given and given off in health care privacy policies are adapted and categorized in an online context. Beyond simply cataloguing of privacy policy statements, the study interprets the quantitative findings to comprehend how these privacy policy statements interact and shape presentation online.

In the academic literature and the business press, there seems to be a lack of guidance and lack of privacy policy assessments to support companies on the Web. This study aims to be informative and applicable for privacy managers at companies in the early stages of developing an electronic commerce strategy, and to academicians studying the evolution of electronic commerce initiatives in the health care business. Rational approaches can be used to deal with the evaluation of privacy policy, and therefore the main features and involved categories and properties for privacy policy metrics are delivered. The contribution of the theoretical privacy frameworks is primarily intended to provide us with a set of standards with which to assess and develop privacy practices even in situations in which no previous privacy policies or privacy regulations exist, and with which to assess other value frameworks when disagreements occur.

The intention in conducting this research is not to embarrass or single out particular health Web sites or to scare consumers away from getting valuable health information; rather it aspires to alert consumers and the industry to

impending threats and problems, so that the industry can develop a more suitable electronic commerce solution.

1.4 Research Process and Empirical Study

Content analysis is a very suitable research technique for studying the privacy practices of health providers because it is an unobtrusive technique which is "*well-developed but underused*" (Neuman, 1994, p. 260), "*with great potential for studying beliefs, organizations, attitudes and human relations. The limited application ..., of content analysis is due more to unfamiliarity with the method and to its historic isolation from mainstream social science than to its inherent limitations*" (Woodrum, 1984, p. 1). Additionally, content analysis was selected because it is an objective and systematic research technique suitable for making replicable and valid inferences from data to their context (Kolbe and Burnett, 1991). Content analysis examines expressed privacy policy statements and an "*objective analysis of messages ... is accomplished by means of explicit rules*" (Berg, 1998, p. 224). These rules are used to "*classify the signs occurring in a communication into a set of appropriate categories*" (Janis, 1965, p. 55). Content analysis, which is used to provide information about the thematic content of communications and about the assertions found in them, "*will probably turn out to be the most productive*" (Janis, 1965, p. 67).

Content analysis is a suitable technique for analyses of secondary data. Although secondary data is usually not used as sources of data in quantitative studies, it plays an essential role in content analysis (Strauss and Corbin, 1990, p. 48). Secondary sources are sources of data that has been produced by others, not specifically for the research question at hand (Frankfort-Nachmias and Nachmias, 1996). It could be comprised of a variety of materials like biographies, diaries, documents, manuscripts, records, and reports, including governments and regulatory agencies, the public reports of companies, articles appearing in the press and other media, published academic research, and the internal documents produced by organizations (Harris, 2001, p.193). Much can be learned about an organization, its structure, and how it functions (that may not immediately be visible in observations or interviews) by studying its reports, correspondence, and memos (Strauss and Corbin, 1990, p. 55). There are many examples indicating the potential of secondary sources. For example, Kabanoff, Waldersee and Cohen (1995) used a wide range of company data to investigate value structures in organizations; Harris (2001) used newspaper

reports to study courage in managerial decision making; Fisher and White (1976) analyzed the content of interview transcripts from audio-recorded discussion groups, using rating scales and coding categories that reliably assessed participants' attitude complexity, positiveness, and behavioral orientations. Secondary data can also be used to provide "*triangulation*", which increases the credibility of research findings using primary data (Cowton, 1998b; Insch, Moore and Murphy, 1997).

The use of secondary data might be challenged on the basis that the privacy policy analysis will only reveal privacy managers' attitude and not that of the prime agents (i.e. all other employees). Although this may be a problem in some research designs, in the "*privacy policy*" case, this is not the case. Privacy policies are valid gauges for content analysis because they capture how organizations express to customers their significant core values, emergent issues, and ongoing activities and practices. The aim of this study is to provide information about the nature of privacy as it is perceived in electronic commerce, and privacy policies are a reflection of that usage. Privacy policies are public organizational records, which are considered to be a form of interaction among customers, organizational constituents and, to a lesser extent, between competing organizations' constituents.

Although the study by Goldman, Hudson, Smith (2000) pointed out that there is inconsistency between the privacy policies and the actual practices of health Web sites, the subsequent FTC (2000) investigation found that many studied Web sites had made changes to their policies in response to the findings of the report. From the customers' perspective, commitments expressed by an organization in their privacy policy must reflect directly on its work practices. This is because privacy policies reflect the external ethical views of an organization and therefore, provide an indication of perceived trustworthiness to those who conduct business with a given organization. Additionally, since the Web site does not conform to its privacy policy, the company may be subject to public outcry or legal action. In terms of online activities, the FTC has the authority to prosecute Web sites that engage in unfair or deceptive practices, such as noncompliance with their own privacy policies[10]. The relationship between expressed privacy policy statements and

[10] In July 2000, the Federal Trade Commission forced a bankrupt Toysmart.com to abandon its plans to sell all of its customers' data to the highest bidder. The firm had promised site users that it would not divulge information gleaned from tracking users' activities on the site, but a court-appointed overseer believed the customer list was a valuable asset that could be sold to help pay off the firm's creditors. In July 2000, Toysrus.com was accused of feeding shoppers' personal information to a data-analysis firm without revealing the relationship to consumers. In response to complaints, Toysrus.com added information to their privacy policy about how customer data is

the company's "*internal*" privacy activities, which do not directly reflect on online customers, are outside the scope of this dissertation.

"*The use of content analysis to study information content on the Web is still at an infancy stage*" (Singh, Zhao and Hu, 2003, p. 71), but content analysis of Web sites has been used in previous research successfully[11]. There "*is no simple right way to do content analysis*" (Weber, 1990, p. 13), but one commonly used procedure involves eight steps (Insch, Moore and Murphy, 1997; Krippendorff, 1980; Weber, 1990; Harris, 2001). Figure 1 presents the used eight-step process (Harris, 2001, p. 194) to be discussed below. Each step is explained further as part of that discussion and in Section 4.1.

treated, but denies that the information is sold to outside vendors. One week after the customer lawsuit was filed, Toysrus.com announced a strategic alliance and restated their commitment to consumer privacy online. (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 5).

[11] See Ghose S. and Wenyu Dou (1998). Interactive Functions and Their Impacts on the Appeal of Internet Presence Sites. Journal of Advertising Research. Vol. 38, No. 2, pp. 29-43; Huizingh E.K. (2000). The Content and Design of Web Sites: An Empirical Study. Information & Management. Vol. 37, No. 3, pp. 123-134.; Perry M. and C. Bodkin (2000). Content Analysis of Fortune 100 Company Web Sites. Corporate Communications: An International Journal. Vol. 5, No. 2, pp. 87-96.; Ellinger A.E., D.F. Lynch, J.K. Andzulis and R.J. Smith (2003). B-to-B Electronic commerce: A Content Analytical Assessment of Motor Carrier Web sites. Journal of Business Logistics, vol. 24, no 1, 2003. pp 199-220.; Singh N., H. Zhao and X. Hu (2003). "Cultural Adaptation on the Web: A Study of American Companies' Domestic and Chinese Web sites. Journal of Global Information Management, Jul-Sep 2003, 11, 3; Papacharissi Z. (2002). The Presentation of Self in Virtual Life: Characteristics of Personal Home Pages. Journalism and Mass Communication Quarterly. Autumn 2002, 79, 3, pp. 643-660.

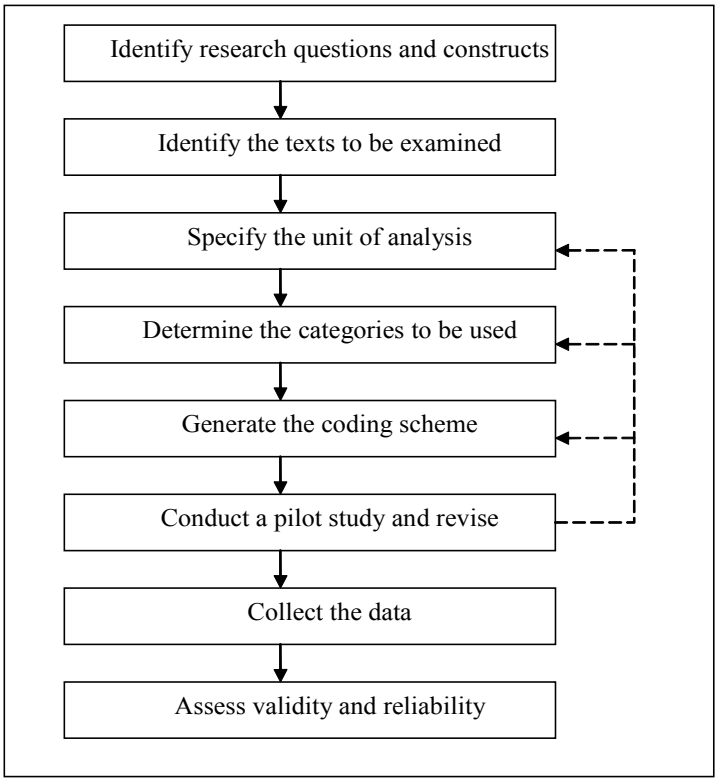

Figure 1: Eight-Step Study Process.

The first step is to identify the research questions to be asked and constructs to be used. The main explorative questions concerning the health care Web sites privacy practices to be investigated in the content analysis were presented in the preceding section.

The second step is to choose the texts to be examined. At the beginning a study, there are many sampling matters that the researchers must think through (see Strauss and Corbin, 1990, p. 179). A decision must be made about the kinds of data to be used. So far, we have discussed why privacy policies are good secondary sources to gather and analyze the most relevant data about practices of privacy matters under investigation. Here, the choice is made on the basis of match – the method of data collection that best captures the kind(s) of information sought. The study used privacy policies found on the health care Web sites as the texts to be examined. This selection process yielded a total sample of 39 U.S.-based health care companies. The health care industry was selected for this study because it is a very sensitive segment where the protection of customers' personal information is not an option but a

necessity. The United States was chosen because there electronic commerce is being taken into use in the health care segment at an increasing pace, and the legal issues of privacy matters are mostly voluntary, as discussed in Section 2.3. It is important to note that that the health care sector and services in these markets are clearly organized and function differently among different countries, thus the results of this study are not valid outside the U.S. For example, the legal category is expected to present different results when applying the framework to international Web sites that are not focused in the U.S. The European directives tend to protect and secure the privacy of the user and not threaten it.

The voluntariness and high sensitivity of the study context makes the assessment of privacy issues more challenging. Security and privacy continue to be major sources of concern for Internet users, and all health care companies in the sample did attempt to reassure potential customers by incorporating security or privacy policy statements into their Web site designs. How vulnerable the subject matter appears to be will vary according to the level of setting at which we operate, but misuse of medical information may be very embarrassing to the customer.

> *"Medical information can be used to deny employment and other opportunities to which a person is entitled, and embarrassment is a form of emotional harm that can have extreme consequences in certain situations." (Thompson, 2001, p. 15).*

It was anticipated that the health care privacy policies would contain material on a wide variety of privacy issues, including management, legal issues, sensitive matters, politics, and community organizations, while also including items of sufficient length for useful analysis. Both these assumptions were tested and confirmed in the pilot study.

The third step is to decide on the type of issue to be counted in the analysis, the so-called "*unit of analysis*". The unit of analysis is the basic unit of text to be categorized as "*the specific segment of content that is characterized by placing it in a given category*" (Holsti, 1969, p. 116). Five units that have been commonly used are word, word sense or phrase, sentence, paragraph, and document, while themes and individual persons are included as options by Berg (1998) and Frankforth-Nachmias and Nachmias (1996).

In some content analysis studies mentioned earlier, the intention has been to determine the frequency with which an individual has used a particular word and in others to compare the coverage of an event in different sections of the media by counting the number of stories or programs devoted to the topic. In the "privacy policy" study the questions to be addressed included the

identification of the typical contents of a health care Web site privacy policy, and typical communication practices of privacy matters. And because "*the unit of analysis should be chosen so that it is consistent with the nature of the research question*" (Harris, 2001, p. 198), phrase (i.e. privacy police statement), which may vary from a couple of words to a sentence, was chosen as the unit of analysis. From this point on, this unit of analysis is referred to as "*item*". Items are the basic building blocks of the presented frameworks.

Content analysis is the analytic process by which items are identified and developed in terms of their properties. The basic analytic procedures by which this is accomplished are: asking questions about the data; and the making comparisons to obtain similarities and differences between each item and other instances of phenomena. Similar privacy items are labeled and grouped to form categories.

It is possible to begin by analyzing privacy policy with a line-by-line analysis. An implication resulting from the research questions and the choice of the privacy policy statement as the unit of analysis is that the data collection must be done by hand using human coders, rather than putting the text through a computer program, because "*computers still have a long way to go to read the meaning of longer text messages*" (Sarantakos, 1993, p. 216). This involves close examination, statement by statement, and even word by word. "*This is perhaps the most detailed type of analysis, but the most generative. (It is also the most tedious if done for too many sessions*)" (Strauss and Corbin, 1990, p. 72). Although the chosen technique is laborious, it is rather widely used. For example, Insch, Moore and Murphy (1997) list seven content analysis studies of management in which the phrase has been used as a unit of analysis.

The fourth step is to determine the categories into which the items are to be divided. Thus a category is a categorization of items. The possible categorizations are discovered when items are compared with each other and appear to pertain to a similar phenomenon. Thus, the items are grouped together under a higher order, a more abstract concept. The term category indicates that certain items are deemed significant because they are repeatedly present or notably absent when comparing privacy policy statement after privacy policy statement, and through the coding procedures they earn the status of categories.

One aim of this explorative study is to discover, name, and categorize privacy policy items and to develop categories in terms of their properties. Consistency is also important. Consistency here means systematically gathering data in each category. Therefore generating the categories early

through "*line-by-line*" analysis is important, because categories become the basis of quantitative analysis. In addition, doing content analysis involves making interpretations. As Diesing (1971, p. 14) points out "*actually scientific knowledge is in large part an invention or development rather than an imitation; concepts, hypotheses, and theories are not found ready–made in reality but must be constructed*." Therefore a comprehensive literature review was conducted using journal articles, textbooks, and the Internet to identify relevant privacy items and categories for evaluating the privacy policy statements of health care Web sites.

The fifth step is to generate the coding scheme. The used procedure "*scans*" a whole privacy policy, the return to the privacy policy statement, phrase, or sentence that appeared significant, important, or of interest. The item should be one we wish think about more deeply. It is important to think about privacy policies analytically rather than descriptively, to generate provisional categories and properties, and to think about generative questions. "*Reduction not only allows analysis, it is analysis, in that clusters and partitions will necessarily follow the analyst's evolving sense of how the data come together and how they address the research questions s/he wishes to answer*" (Huberman and Miles, 1983, p. 285). "*Qualitative methods can be used to uncover and understand what lies behind any phenomenon about which little is yet known*" (Strauss and Corbin, 1990, p. 18), but because "*every qualitative analyst encounters the problem of data overload*" (Huberman and Miles, 1983, p. 285) it is important to generate a coding scheme. This requires not only a set of categories that are "*independent, exhaustive and mutually exclusive*" (Sarantakos, 1993, p. 212), but also the rigorous use of a clear set of coding guidelines (Strauss, 1987). It is important to note that the content analysis procedure should allow for each significant variation in privacy policy statement to be coded in a distinct and consistent manner. In this study, each of the privacy items were coded in accordance with the coding schemes and with guidelines suggested by Strauss (1987), who advises the researcher to ask the data a specific and consistent set of questions and analyze the data minutely.

The sixth step is to conduct a sample or pilot study and revise the categories and coding schemes as needed. The presented empirical study includes four "*phases*". Table 1 presents the Study Schedule. The first phase of the research was collaborative by nature. It was performed as a pilot study by two researchers and one graduate student, and consisted of the 23 health care Web sites' privacy policies. It resulted in a draft version of the data and an evaluation instrument. The author joined the research team in the summer of

2001. Prior to that the graduate student had departed. First, all three remaining researchers worked in teams. When working with a team of researchers, it is important that each member attend the analytic sessions (Strauss and Gorbin, 1990, p. 189), and our research practice followed that principle, thus keeping one another on track. Each member received copies of any draft results of privacy policy analyses. Project meetings continued until all researchers were confident that all members of the team were fully conversant with the operational definitions and evaluation procedures.

To redevelop the instrument and make a check on the reliability of the evaluation process, several randomly selected Web sites and other documents were also evaluated by the author, for example, the privacy policy of URAC[12] Web site and a portion of the European Union Directive 95/46/EC[13], and a European Recommendation[14] addressing Internet privacy. New potential problem areas were identified and discussed with the research team members until a consensus was reached and the necessary definitional and procedural changes of instruments and technique could be made.

To increase objectivity, the first phase of the Web site privacy policy evaluation was reviewed (i.e. second phase) by the author in the fall of 2001. New items and categories found were brought back to the research group and shared. It was important that each member knew about the new categories and privacy policies being investigated. The team met regularly and frequently to analyze portions of privacy policy data until the spring of 2002. Working this way as an analytic unit, all members remained firmly within the same conceptual frameworks. The research team provided written operational definitions for some categories and items in the instrument and used objective coding procedures for conducting the privacy policy evaluations. Later all researchers worked separately, but in the second phase it was important that everyone read all the resulting memos, otherwise the full resources of the team could not be applied the data nor could analytic consistency be so easily obtained.

---

[12] URAC is the Utilization Review Accreditation Commission (URAC), a nonprofit accreditation organization.

[13] DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[14] RECOMMENDATION No R (99) 5 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES FOR THE PROTECTION OF PRIVACY ON THE INTERNET GUIDELINES FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE COLLECTION AND PROCESSING OF PERSONAL DATA ON INFORMATION HIGHWAYS (adopted by the Committee of Ministers on 23 February 1999, at the 660th meeting of the Ministers' Deputies) http://cm.coe.int/ta/rec/1999/99r5.htm

After the second phase, the other researchers focused on the privacy policies of the financial sector (Anton, Earp, Bolchini, He, Jensen, and Stufflebeam, 2003). The author focused more closely on health care Web sites. The third phase of the empirical study included 16 health care Web sites. This data collection phase was started in the spring of 2002, and the initial evaluation was completed in the fall of 2002. The empirical studies during Phase 1 and Phase 2 have been done based upon the use of the Goal-Based requirements Analysis Method – GBRAM (Anton, 1997; Anton and Potts, 1998)[15], but during Phase 3 and Phase 4 the author used the content analysis as described in this dissertation.

The analytic process itself is a source of theoretical sensitivity[16], which is needed when making analyses. "*Theoretical sensitivity has two sources. First, it comes from being well grounded in the technical literature as well as from professional and personal experience. You bring this complex knowledge into the research situation. However, theoretical sensitivity is also acquired during the research process through continual interactions with the data – through your collection and analyses of the data*." (Strauss and Corbin, 1990, p. 46). Insight and understanding about a phenomenon increase as a researcher interacts with data. This comes from collecting data, making comparisons, making propositions, developing small theoretical frameworks (mini frameworks) about items and their relationships. In turn, the researcher uses these to re-examine at the data. Often, one idea or insight sparks another, directing a researcher to look more closely at the data, to give meaning to words that seemed previously not to have meaning, and to look for situations that might explain what is happening here. (Strauss and Corbin, 1990, p. 43). For this thesis, every effort was made to ensure that each of the 39 privacy policies in the sample was evaluated using the same instrument, the same

---

[15] The GBRAM is a methodical approach to identify system and enterprise strategic and tactical goals as well as requirements. Goals are the objectives and targets of achievement for a system. The method suggests goal identification and refinement strategies and techniques through the inclusion of a set of heuristics, guidelines and recurring question types. Five sets of heuristics are included: identification heuristics, classification heuristics, refinement heuristics, elaboration heuristics and conflict identification/resolution heuristics (see Antón A.I., 1997). Goal Identification and Refinement in the Specification of Software-Based Information Systems, Ph.D. Dissertation, Georgia Institute of Technology, Atlanta; and Antón A.I. and C. Potts (1998). The Use of Goals to Surface Requirements for Evolving Systems, Int'l Conf. on Software Engineering (ICSE '98), Kyoto, Japan, pp. 157-166, 19-25 April 1998). In software engineering, goal-driven approaches for requirements focus on why systems are constructed, expressing the rationale and justification for the proposed system. See Lamsweerde A. van (2001). Goal-Oriented Requirements Engineering: A Guided Tour, IEEE 5th Int'l Symp. on Requirements Engineering (RE'01), Toronto, Canada, pp. 249-261, 27-31 August 2001.

[16] "Theoretical sensitivity refers to the attribute of having insight, the ability to give meaning to data, the capacity to understand, and capability to separate the pertinent from which is not." (Strauss and Corbin, 1990, p.42).

theoretical knowledge and the same research technique and therefore, all studied privacy policies were reviewed in the spring of 2003 (the fourth and final phase).

Table 1: Study Schedule.

Phase	***Schedule***	***Number of Web sites***	***Done by***	***Research Technique***	***Reported***
1	Spring 2001	23	Anton, Earp, and Reeves	GBRAM	Anton, Earp and Reeves, 2002
2	Fall 2001	23 + URAC and EU-Dir.	Anton, Earp and Järvinen	GBRAM	Earp, Anton, and Järvinen, 2002 Järvinen, Earp, and Anton, 2002
3	Fall 2002	16	Järvinen	Content Analysis	
4	Spring 2003	39	Järvinen	Content Analysis	Järvinen, 2003a; 2003b; Dissertation

Since sensitivity usually increases with time, an interesting and important feature of the content analysis study is that one can sample from previously collected data, as well as from data yet to be gathered. "*It is not unusual in the early stages of a research project, for investigators to overlook or fail to pick up on the significance or meaning of certain events or episodes, because of a lack of theoretical sensitivity. Later, when developing new insights, an investigator can legitimately return to the old materials, and recode them in light of additional knowledge*." (Strauss and Corbin, 1990, p. 181).

The other reason for reviewing the whole sample was to minimize the risk presented by major site changes. This dissertation refers to health Web sites as they existed during the study presented in Table 1. Two companies were found to not have operational Web sites during the fourth data evaluation period. In those cases, the author has used the results of the evaluation performed in the fall of 2002. Given the ever-changing nature of the Internet, it is possible that the organization or practices of these Web sites have changed since that time. The Web sites are presented in more detail in Section 4.1.

Some take the view that content analysis is a quantitative technique (Silverman, 1993; Neuman, 1994), and evidence of the use of quantitative analysis of printed material goes back to a religious dispute in eighteenth century Sweden, while Max Weber proposed a large scale content analysis of the press as early as 1910 (Krippendorff, 1980). For others (Berg, 1998; Insch,

Moore and Murphy, 1997; Sarantakos, 1993), it has elements of both the qualitative and quantitative approaches in that the counts of textual elements that emerge from the first stage of the analysis "*merely provide a means of organizing, indexing and retrieving data . . . This offers, in turn, an opportunity for the investigator to learn about how subjects or the authors of textual materials view their social worlds*" (Berg, 1998, p. 225). This study used a wide combination of qualitative and quantitative methods. The two types of methods can be used effectively in the same research project (Strauss and Corbin, 1990, p. 18), and the most published work relating specifically to health Web sites has focused on descriptions of individual Web sites rather than on assessments of entire and divided business segments. This research was undertaken to provide an overview of Web site privacy issues within the health care industry as a whole, but also to provide an overview of privacy aspects and issues found in five health care business segments: pharmaceuticals, health insurance, online drugstores, medical institutes, and general health information.

Measures, a well-defined sampling design and system of categories, and adequacy of operational definitions are all necessary to obtain valid results from content analysis (Berelson, 1952: Kolbe and Burnett, 1991). The Randall and Gibson review found "*surprisingly little concern for either validity or reliability of the research instruments"* (1990, p. 462), while other authors note that assessment of construct validity has been frequently missing from empirical research studies in business and corporate ethics (Weber, 1992; Cowton, 1998a; Ford and Richardson, 1994), or indeed in empirical qualitative studies generally (Silverman, 1993). The eight-step process is designed to assess validity and reliability, which will be considered in Section 4.1.

1.5 Overview of the Thesis

Discovery is the primary focus of this explorative study and data collection, and the analyses and the associated theoretical sampling are structured to allow for this. This study explores the relationship of Internet electronic commerce, and the concept of informational privacy is at the center of this relationship perspective. The study concentrates on privacy issues and problems in two main interests; namely the Internet customer and the health provider. A theoretical assumption for the privacy problem is that the components (customers' interest, companies' interest) are not in balance. A

key detail of the Internet is that there is no such thing as "*absolute privacy*". The evolving trend toward new business practices and services has resulted in increased information collecting, using, and sharing among organizations. Unfortunately, such information practices may conflict with consumers' desires to be shielded from unauthorized use of their personal information. "*People often believe they are invisible and anonymous online, but they are often exposing their most sensitive health information to online health care sites that are not required by law to protect the information or keep it confidential. The potential for abuse is enormous*." (Choy, Hudson, Pritts and Goldman, 2001, p. 25).

Empirical and theoretical studies were included in the research design of this dissertation to prevent what Weaver and Trevino call the "*parallel approach*" to business ethics research, where normative inquiry becomes "*too abstract, too idealistic, to be of any practical value*", by avoiding any contact with empirical research (1994, p. 132). Although "*privacy*" was not normative in its intent, and that may place a limit on the relevance of the Weaver and Trevino analysis, the empirical component was included in the overall research plan to avoid the division between frameworks and practice, which they see as both the result and the basis of the parallel model. An investigation of the way in which the "*privacy*" is understood would provide a "*reality check*" on the conceptual development. To systematize and solidify connections, a combination of inductive and deductive thinking is used, in which it constantly switches between asking questions, generating propositions, and making comparisons.

In order to discover privacy items in privacy policies we need theoretical sensitivity, the ability to 'see' with analytic depth what is there. "*Literature can be used to stimulate theoretical sensitivity by providing concepts and relationships."* (Strauss and Corbin, 1990, p. 50). Later in the research project, theoretical sensitivity develops from working with the privacy policies themselves. But in the early analytical stages, we need ways of opening up our thinking about the phenomena we are studying.

The main focus of Section 2 and Section 3 is to determine the demands for a good privacy policy on a Web site. Section 2 discusses the instrumental, intrinsic, and core value of privacy. Furthermore, the legal issues are presented. "*Knowledge of existing theories can also provide ways of approaching and interpreting data*" (Strauss and Corbin, 1990, p. 51), and therefore the nature of privacy issues, privacy theories and principles are presented. Section 2 presents the existing privacy theories and considers how they apply "*to new and varied situations, as differentiated from those*

situations to which it was originally applied." (Strauss and Corbin, 1990, p. 51). The convenient framework of privacy in the context of the Internet is presented. The privacy framework acknowledges an important distinction among the different interests affected by electronic commerce and the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings.

Section 3 discusses business interest and customer interest. To determine whether the privacy practice or policy of a Web site actually violates the privacy of customers, it is important to describe useful privacy frameworks as precisely as possible. Such frameworks should enable us to differentiate "*good privacy policies and practices*" from "*bad ones*". An adequate privacy framework should also provide some procedure for determining whether certain kinds of practices are vulnerable or not. This understanding should help us to develop privacy policies and practices to be more suitable for electronic commerce.

Although we need to analyze before we can formulate and justify a policy and practice, the process of discovery often comes in the reverse order. We know that computing technology is being employed in a given situation, but we are puzzled about how it should be used. For example, should a company be allowed to use a customer's personally identifiable information without the consent of the customer in a special situation? Or should the government be allowed to censor some information on the Internet? Initially, there may be no clear policies on such matters. They never arose before, and there are policy vacuums in such situations. Sometimes it may be simply a matter of establishing some policy, but often one must analyze the situation further. Is email in the workplace more like correspondence on company stationary in company files or more like private and personal phone conversation? (Moor, 1998, p. 17).

The interactivity features of the Internet provide companies with many opportunities for online management so that the customers can make the most convenient choices in terms of their own needs and values from a number of alternatives. For example, some online services allow the users to alter parameters. What one user considers a privacy invasion may be a valued feature or service to another user. Sufficient flexibility should be included to define an adequate privacy model in the context of the Internet service. A variety of possible scenarios are presented and the balanced privacy model is determined. In that model, customer privacy (Privacy-on-Demand function) is related on the function of service (Service-on-Demand function).

Section 4 presents the empirical study. It provides an overview of communications practices and typical contents found in 39 privacy policies of health care Web sites in five health care segments: pharmaceuticals, health insurance, online drugstores, medical institutes, and general health information. Each privacy policy statement was examined and all privacy-related items were analyzed to determine what communications practices for privacy matters and what typical privacy categories and properties are found in health care Web sites.

The usage situations and factors affecting privacy issues on both the customer and organizational side are discussed in the context of different categories where the major category scheme (i.e. protective and vulnerability category), visibility category scheme (i.e. visible and invisible category), and modularity category scheme (i.e. legal, business, contractual, social, and technical category) have a central role. Organizations should have a sound privacy policy and practices, but the company should also be able to convert customer information into useful knowledge. Privacy seal programs may arise as a solution to the Internet business, and it may be central role of such institutions and therefore privacy programs are presented and analyzed.

The ability to provide differentiated, consistently superior customer service on the Internet will be crucial to the survival of health care companies, but the study findings submit that health providers' Web sites are still in the relatively early stages of their privacy issue evolution. These shortfalls may be partly due to the speed with which many companies have established an Internet presence. It is also relatively easy to set up a Web site, but far more difficult to create a web-based business model (Ghosh, 1998). However, as customer demands continue to rise and the availability of informational and interactive Web site content continues to proliferate, the bar for acceptable performance by health providers will continue to rise.

The management of organizational privacy practice should successfully anticipate many changes. The development of privacy practice in the turbulent environment of electronic commerce can be crystallized in one question: "*What ought to be covered and measured?*" Many system-design and assessment methods provide the basis for investigating how information systems should be planned, designed, implemented, and evaluated, but the development of the Internet cannot be easily distinguished from the broader perspectives related to developing services as a whole, including ethical aspects.

The attempt to find one general measure for global privacy policy fails – there are too many situation-dependant aspects to consider. Privacy matters

are deeply situation-dependent issues and cannot be found by applying a predefined list without considering the situation widely. A privacy problem may arise in a specific situation, and it may occur as the result of an unpredictable incident. Privacy constantly includes a large number of evolving situations that are difficult to conceptualize clearly and for which is it hard to find justified practices. Therefore, privacy involves more than rote application of existing norms. Privacy is widely related to computer ethics generally. It includes features and problems that are alike. "*No other technology, as revolutionary as it may be for a given area, has and will have the scope, depth, and novelty of impact that computing technology has and will have*." (Moor, 1998, p. 17). But if privacy issues are not routine, how can it be done at all? Retreating to a position of Cultural Relativism will not solve the dilemma. In accordance with this view local customs and laws determine what is right and wrong. "*According to cultural relativism, ethical issues must be decided 'situationally' on the basis of local customs and laws*." (Moor, 1998, p. 18). Problems place us in such a position with regard to privacy issues of electronic commerce. Because information and knowledge easily cross cultural, institutional, organizational, and many other boundaries, the challenges of privacy issues are intractable. Additionally, Internet application and its context may be so novel that there are no convenient customs or laws established anywhere to cope with privacy issues. A vacuum in terms of privacy practice may occur in every culture. The different categories and the balanced privacy model discussed in this dissertation provide a good foundation and mechanism to evaluate and develop privacy issues in more detail. In addition, this dissertation proposes an approach, the layered privacy model, to manage the privacy practices of Internet companies. It is developed on the basis of the empirical part of the study and the presented theoretical frameworks to avoid a parallel approach.

This dissertation showed one possible technique to assess the content and communication practices of privacy policies in health care Web sites. To answer research questions, a content analysis of expressed online privacy policies was conducted. The content analysis is described and the results are reported, which is followed by discussions and conclusions. Future study could test whether the presented technique, the balanced privacy model, and the layered privacy model are also suitable in a wider context. To enhance the reliability of the technique, the author urges future researchers to replicate this study in other communities. However, the author believes that this dissertation will be informative and applicable to privacy managers at companies in the early stages of developing an electronic commerce strategy and to

academicians studying the evolution of electronic commerce initiatives in the health care business.

2 ISSUES OF PRIVACY

As in any research, there is a need to ensure that a theoretical basis can be identified which underlies the questions being asked and any constructs which are being tested (Harris, 2001, p. 192), and therefore, this chapter discusses the instrumental and intrinsic value of privacy. Discussion emphasizes the core values, because they provide a common value framework. This global entity of core values gives us reasons to prefer some privacy policies and practices over others. Additionally, a variety of privacy theories, principles and law statutes are presented.

When the ethical problems involving the Internet are considered, none is more paradigmatic than the issue of privacy. Given the ability of information technology to widely gather, endlessly store, cheaply transfer,efficiently sort, and effortlessly locate information, we are justifiably concerned that the Internet world may provide the means to invade our privacy and reveal information that is harmful to us. This is not to say that all information on the Internet is a breach of privacy, but it is used to point out how the same information, which has technically been public for a long time, for example, listed telephone numbers and a map of a residential area based on the address, can, as Moor (1997, p. 27) points out, "*dramatically change levels of accessibility practically speaking when put into electronic form on computer networks*." We are, however, reluctant to give up the advantages and the services of the Internet. We appreciate the easy access to the Internet services when checking health information, buying the drugstore items, and many other things. The number and kinds of applications on the Internet increase dramatically each year, and the impact of the Internet is felt around the planet.

The interest in privacy issues is not a new matter. In early times, the U.S. law only protected against physical interference with life and property, and later the scope of these legal rights broadened. For a hundred years there has been the feeling that the change in society and technology must afford some remedy for the unauthorized use of tangible and intangible property. Since the era of newspaper and photography, privacy has been considered an important issue.

> *"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the*

> *common law, in its eternal youth, grows to meet the demands of society. ... and now the right to life has come to mean the right to enjoy life—the right to be let alone, the right to liberty secures the exercise of extensive civil privileges; and the term property has grown to comprise every form of possession—intangible, as well as tangible"*
> *(Warren and Brandeis, 1890).*

The development of the law and the change of attitude were natural because the life of a person includes much more than physical things. Intangible property and the right to privacy also demanded legal recognition. The right to privacy is usually discussed as a branch of tort law, but functionally it is really a branch of property law. The earliest American judicial recognition of an explicit right to privacy came in a case where the defendant had used the plaintiff's name and picture in an advertisement without the plaintiff's consent (Posner, 1992, p. 43).

2.1 Privacy

To determine whether a particular technology actually violates the privacy of individuals, it is important to describe the term privacy. Such a focus should enable us to differentiate privacy from many other concepts.

2.1.1 Background

Stacey Edgar (1997) interprets privacy as a straightforward extension of Lockean non-interference rights and Kantian autonomy, and then offers some indicative examples of how computers have been used to violate privacy. Thus, privacy seems to be a very simple issue. On the one hand, privacy seems to be something of very great importance and something vital to defend, and, on the other hand, privacy seems to be matter of individual preference, culturally relative, and difficult to justify in general (Moor, 1997, p. 28). This is because privacy is a social, cultural, and legal concept, all three aspects of which vary from country to country (Gotlieb, 1995, p. 156). Herman Tavani states that privacy, which is often associated with, and sometimes described in terms of, liberty, autonomy, solitude, and secrecy is a concept that is not easily defined (Tavani, 1999a, p. 137). "*Unlike privacy*," Thompson writes that

(2001, p. 15) "*secrecy appears to have a tight connection to information*." If something is secret, there is at least one person to whom the information is not known. "*While confidentiality continues to be an important ethical problem for computer professions, and while security is an increasingly important technical issue, privacy is a red herring*." (Thompson, 2001, p. 14).

When we consider privacy on the Internet, Moor (1998, p. 16) points out that "*one often finds oneself in a conceptual muddle"* and "*the issues are not trivial matters of semantics*." For example, "*many Americans know that violation of copyright is a crime, and many believe that violation of their privacy should be a crime too. Why is distributing a corporation's software without its permission called 'piracy,' while distributing a person's information without permission is called 'sharing'?"* (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 11).

Yet there are cases when general knowledge of private matters does not breach persons' privacy in any morally significant way. A person's religious practices (or health information) may be widely known, but that in no way makes them less private. Thompson (2001, p. 15) points out that "*having information about a person's religious practice may make it possible for someone to violate that person's privacy by discriminating for or against them in an inappropriate way."* Such information is widely available in most societies, and Thompson continues by writing "*the significance of such information lies not in simple knowledge of it, but in its further use*". If someone's health status is shared through email or health providers use a customer's personally identifiable information to send medicine samples without the customer's consent, the consequences may be significant.

2.1.2 Instrumental and Intrinsic Value

A variety of arguments have been put forth to defend the value of personal privacy, and it will be useful to continue by distinguishing privacy as an instrumental good from privacy as an intrinsic good. Moor (1997) justifies privacy using those two different perspectives: instrumental and intrinsic. Instrumental values are those values that are good because they lead to something else which is good. Intrinsic values are values that are good in themselves. Moor states that "*philosophers since Aristotle have pointed out, that some things, such as health, have both instrumental and intrinsic value."* Moor (1997, p. 28).

Privacy has instrumental value and this is its most common justification. Privacy offers us protection against harm. Moor (1997, p. 28) points out that in some cases "*if a person's medical condition were publicly known, then that person would risk discrimination."* If the person tests HIV+, an employer might be reluctant to hire him and an insurance company might be reluctant to insure him. These kinds of example are easy to find, and they all indicate that privacy has instrumental value. Moor (1997, p. 28) writes that "*to justify the high instrumental value of privacy we need to show that not only does privacy have instrumental value but that it leads to something very, very important.*" One of the most well-known attempts to do this has been given by James Rachels. Rachels suggests that privacy is valuable because it enables us to form varied relationships with other people (Rachels, 1975, p. 351). Privacy also enables us to form intimate bonds with other people that might otherwise be difficult to form and maintain in public. Charles Fried claims that privacy is instrumentally valuable while Fried (1970, p. 55) states that privacy is essential or necessary for human ends such as trust and friendship.

In a society where individuals have no privacy, Fried argues, friendships, intimacy, and trust cannot develop. If we want such relationships, we must have privacy. Moor (1997, p. 28), however, writes that the need to relate to others differently may not ground privacy securely "*because not everyone may want to form varied relationships and those who do may not need privacy to do it*." This is based on the principle that some people simply do not care how others perceive them.

So far, we have seen that some arguments present privacy as an instrumental value and some arguments tie privacy more tightly to autonomy. Privacy is understood to be not just a means of autonomy but a part of the very meaning of this term. We don't seek privacy in order to get autonomy, but as Johnson (1994, p. 89) has suggested "*autonomy is inconceivable without privacy*." Autonomy is not just one among many values, i.e. autonomy is fundamental to what it means to be human and to our value as human beings. Johnson suggests that privacy is necessary for diversity of relationships and privacy is an essential aspect of autonomy. Finally, she concludes that privacy might best be understood as "*power*" in modern, democratic societies (Johnson, 1994, p. 89).

"*Assuming that autonomy is intrinsically valuable and privacy is a necessary condition for autonomy we have the strong and attractive claim that privacy is a necessary condition for an intrinsic good*." (Moor, 1997, p. 28). But, as Moor asks, is it true that autonomy is inconceivable without privacy? Suppose an online pharmacy collects information about customer purchases.

Normally, customers recognize the collection process when he/she fill medicine prescriptions online. Consider the situation in which company is not (directly) harming customers. They don't share the information with anyone else or take advantage of customer in any way whatsoever. Customers have complete autonomy, just no privacy. Thus, it follows that privacy is not an essential condition for autonomy. It is conceivable to have autonomy without privacy.

Thompson points out (2001, p. 15) that "*The Warren and Brandeis conception of privacy is clearly intended to articulate a conception of privacy that is more than instrumental value ... privacy as Rachels*[17] *describes it is at least a Rawlsian primary good – a good essential to the realization of any person's conception of the good life*." Thompson (2001, p. 18) continues that "*I am more inclined to think of privacy as a primary good than as a fundamental liberty or as a merely instrumental good*."

To justify the importance of privacy more exactly, we can continue by asking whether privacy is a core value.

2.1.3 Core Value

Core values are set of values that are shared by most, if not all, humans and are familiar to all of us. They are shared and fundamental to human evaluation, for example, life and happiness are two of the most obvious. It is possible to test for a core value by asking whether it a value that is found in all human cultures. The core values provide standards with which to evaluate the rationality of our actions and policies. They give us reasons to prefer some courses of action over others. They provide a framework of values for judging the activities of others as well (Moor, 1997; Moor, 1998).

Moor (1998, p. 20) states that "*as we become acquainted with other cultures, differences often strike us. The members of other cultures eat different meals, wear different clothing, and live in different shelters. But at a more abstract level people are remarkably alike.*" So we may find the habits of others to be even dubious, but after investigation we don't find them to be unintelligible. "*This doesn't make the practices of others uncriticizable, any more than our own are uncriticizable but it does make them understandable*" Moor (1997, p. 29). Moor continues that "*the concept of privacy has a*

[17] In a 1975 article, James Rachels lists several cases where "information about a person might provide someone with a reason for mistreating him in some way".

distinctly cultural aspect which goes beyond the core values. Some cultures may value privacy and some may not." He writes that different cultures and different individuals within a culture may articulate the core values differently in their assessments of values, and some values of one individual may change over time, but such relativity is compatible with rational discussion of privacy issues (Moor, 1998, p. 20).

"*Possessing core human values is a sign of being rational but it is not a sufficient condition for being ethical. To adopt the ethical point of view one must respect others and their core values*." (Moor, 1998, p. 20). We can acknowledge the difference in values among people and among cultures and still engage in rational discussion about the best policies for using information and information technology. "*We are entering a generation marked by globalization and ubiquitous computing. The second generation of computer ethics, therefore, must be an era of global information ethics. The stakes are much higher, and consequently considerations and applications of Information Ethics must be broader, more profound and above all effective in helping to realize a democratic and empowering technology rather than an enslaving or debilitating one*." (Bynum and Rogerson, 1996, p. 135).

The core values are emphasized because they provide a common value framework, a set of standards, by which it is possible to assess the activities of different people and different cultures. This global entity of core values gives us reasons to prefer some privacy policies and practices on the Internet over others. The core values allow us to make transcultural judgments. Though there is a common framework of values, there is also room for much individual and cultural variation within the framework. Moore (1997, p. 29) calls the articulation of a core value for an individual or a culture the "*expression of a core value*".

Maybe privacy is not a core value per se, but it is deeply linked to the value of security. Gotlieb (1995, p. 168) points out that "*What must be secured in every civilized and free society is, of course, security of person*." Protection from strangers who may have goals antithetical to our own is sought, and all cultures need security of some kind because without protection species and cultures don't survive and flourish. "*As societies become larger, highly interactive, but less intimate, privacy becomes a natural expression of the need for security."* (Moor, 1997, p. 29). In particular, a highly computerized culture where lots of personally identifiable information is manipulated, stored, and transferred, it is almost inevitable that privacy will emerge as an expression of the core value, security.

In summary, the justification of privacy is firm because privacy can be grounded instrumentally and intrinsically – instrumentally, in support of the core values, and intrinsically, as an expression of security and more. Because privacy is instrumental in support of the core values, it is instrumental for important matters. Moreover, because privacy is an expression of the core value of security, it is a critical, interlocking member of our systems of values in our increasingly electronic culture. If an online company collects a lot of personally identifiable information without consent (which doesn't harm its customer when it collects, stores, and manipulates), it nevertheless seems to be doing something wrong intrinsically. The subjects' security is being violated by the company even if no other harm befalls the person. The seminal article of Warren and Brandeis (1890) initiated the view that privacy is a positive good, and that individuals have an interest in maintaining a political right to privacy. Privacy is also a necessary means of support in a networked electronic commerce, and thus, privacy is well grounded for this study. People have a basic right to protection, which, from the viewpoint of the global electronic commerce, includes privacy protection.

The following considers some useful distinctions to help avoid some misunderstandings about the nature of privacy. Natural and normative privacy and possible attitude changes regarding privacy are discussed. Privacy cannot be sufficiently considered without social aspects, and therefore social and personal interest is also discussed.

2.1.4 Natural, Normative, and Informational Privacy

The term "*privacy*" is sometimes used to designate a situation in which people are protected from intrusion or observation by natural or physical circumstances. Moor (1997, p. 30) states that "*someone spelunking by herself would be in a naturally private (and probably dangerous) situation*." Additionally, privacy rights are intended to protect a sphere of activity, often a physical place but sometimes an interpersonal relationship, from intrusion by government and other third parties, "*the right to be let alone*" (Warren and Brandeis, 1890). Beyond that, privacy can be vague and highly situational (Thompson, 2001, p. 15).

In addition to natural privacy there is normative privacy. A normatively private situation is a situation protected by ethical, legal, or conventional norms. Consultations with a doctor would be normatively private situations. Many normatively private situations can be naturally private as well. If an

unauthorized entry is made into a normatively private situation, "*privacy has not only been lost, it has been breached or invaded.*" (Moor, 1997, p. 30).

> *"We quickly come to the point that privacy is not merely a matter of this or that person, object, or bit of information, but really applies in systematic ways throughout a society in accord with the norms of that society and, probably, its laws. It is reasonable to expect privacy for actions inside one's home (subject to certain qualifications) because we live in a society where domestic privacy is valued and the laws that protect it are reasonably drawn" (McArthur, 2001, p. 125).*

If we put conceptions of privacy together with distinction between normative and natural privacy, we get a situation-dependent issue of privacy:

> *"An individual or group has normative privacy in a situation with regard to others if and only if in that situation the individual or group is normatively protected from intrusion, interference, and information access by others."*
> *(Culver, Moor, Duerfeldt, Kapp, and Sullivan, 1994, p. 6).*

The general term "*situation*" is deliberately used in this dissertation because it is broad enough to cover many kinds of privacy: private locations such as an electronic patient record in a database, private relationships such as an electronic prescription to one's pharmacy, and private activities such as the utilization of computerized health information. The term "*situation*" covers also role, time and place-dependant issues in this study. For instance, if a nurse uses an information system for the enrollment of a patient and processes a patient's health care treatment using the older information of the patient, then the employee is not invading the patient's privacy. She is allowed in this situation and working role to investigate the patient's case record. However, if that same employee were to "*open*" that same patient's case record after hours just to browse around, then the employee would be violating the patient's privacy although the employee may gain no new information. The nurse has legitimate access in the first situation but not the in the second.

New technology changes the situation of what we may consider private and addressing information-related privacy concerns, including access to personally identifiable information (PII) stored in databases. Many analysts use the expression "*informational privacy*" or "*information privacy*" to refer to a distinct category of privacy concern. Informational privacy is a category of privacy with a set of issues that are distinguishable from privacy concerns related to intrusion and interference (Tavani, 1999a; Tavani, 1999b).

2.1.5 Social and Personal Interest

Williamson (2000, p. 596) presents the social analysis, in the setting of economics of institutions, within four levels: embeddedness, institutional environment, governance, and resource allocation. The top level is the social embeddedness level where the norms, customs, mores, and traditions are located. Ethical issues, like privacy, play a large role at this level. Williamson states that institutions at this level change very slowly – on the order of centuries or millennia – whereupon he states that many of these informal institutions have mainly spontaneous origins – "*which is to say that deliberative choice of calculative kind is minimally implicated*". Institutions are adopted and thereafter display a great deal of inertia. *"…the resulting institutions have a lasting grip on the way a society conducts itself.*" Insular societies often take measures to protect themselves against *"alien values*" (Williamson, 2000, p. 598).

Privacy issues of electronic commerce are, however, more complex and temporary by nature. In this dissertation privacy issues are not adopted on the basis of the history, because the prevailing situation matters a lot. This shows that our role is an important factor. It will largely turn on whether we are subject to a threat or not. We are ready to sacrifice all levels of privacy in return for some level of help in the case. It is difficult to find any opposing arguments. Another equal example of natural privacy is an accident. In these kinds of cases, the most accurate and exact information and knowledge available is the best by any means. We are very eager to give away a lot of our privacy in return for some level of urgent aid when needed. This view is also consistent with exchange theory.

The radical attitude change of normative privacy is also possible as the result of an unexpected event[18]. According to a study published one week after the terrorist attack of September 11 by Pew Research Center, about half of Americans said they are willing to sacrifice civil liberties to curb terrorism, as opposed to the 29 percent who were in 1997. Following the attack, there were several different legislative proposals in the U.S. and some of them were very reactionary and very invasive (Hempel, 2001). There was no sign of Williamson's "*great deal of inertia*".

[18] This is discussed in more detail in Järvinen O.P. (2003) Revision of Privacy Policy: Five Perspectives and ONION-model. People and Computers: Twenty-one Ways of Looking at Information Systems. (ed. Järvi, T. & Reijonen P.) TUCS General Publication, No 26, June 2003, pp. 167 – 184.

The preceding attitude change stems from the personal and social costs of sabotage and the concomitant personal and social benefits of tight security. But there is almost a paradox about our feelings in this matter. For the sake of my safety, I would like all others' transactions monitored to eliminate any possibility that they will be able to damage society. At the same time, I would prefer that my transactions not be monitored. My wish to maintain privacy for my personal transactions is, however, unreasonable against the generalization of everyone's wish for their safety. "*In isolation my desire for privacy is reasonable; it only becomes unreasonable in the contemporary social context."* (McArthur, 2001, p. 125). Regan (1995, p. 213) notes that when we frame the debate simply in terms of how to balance privacy interests as an individual good against interests involving the larger social good, support for those interests believed to benefit the latter good will likely override concerns regarding individual privacy. If the monitoring of transactions would add security in a community or would raise that community's standard of living, then a decision to add monitoring would likely be perceived as yielding a greater overall good than would a decision to protect the privacy of individuals. "*Marxian, Weberian and Foucoldian social theories each stress the state's growing capacity to maintain surveillance over its population as an expression of social power"* (Thompson, 2001, p. 14). David Lyon and Elia Zureik (1995) also describe an approach to privacy based on sociological theories of social control and the expansion of state power.

In the U.S., the attitude change regarding normative privacy was, however, so radical and fast that some professionals started to halt the whole process and were worried about the final result. Deb Aikat, a professor at UNC-Chapel Hill who is specialized in the Internet and society, stated that:

> *"The first thing that comes to my mind is, now it is getting so easy to track everything. Now, you could even get logs of what people are doing on their Web pages."*
> *(News and Observer, 24.9.2001).*

State Senator Eric Reeves, who is chairman of the senate Information Technology Committee, said he has worried in the past few days about how escalating calls for increased surveillance will affect people's sense of privacy.

> *"The rhetoric I'm hearing indicated to me that there may be some very constitutional-law issues at stake here. We must be very careful at all times, that we have to respect people's reasonable expectations of privacy. The public's opinion will be on the side of increased surveillance right now, because nobody thinks of themselves as being a terrorist. So there may be some*

> *very well-intentioned laws coming in the next several months. ... But an overly broad law that over time starts to ensnare law-abiding Americans – that may be the situation we are heading toward."*
> *(News and Observer, 24.9.2001).*

The preceding statement reflects the idea of the "*great deal of inertia",* but it includes also elements of the threat of overly broad normative law that contains the possibility for misinterpretations.

2.2 Privacy Frameworks

The main focus of this section is to present existing privacy theories and consider how they apply to the context of the Internet. In order to determine whether the Web site privacy policy statement (i.e. category item) actually violates the privacy of customers, it is important to describe useful privacy frameworks. Such frameworks should enable us to differentiate "*good privacy policies"* from "*bad ones*". They should also help us to determine what is required to have privacy on the Internet for determining whether certain kinds of personal data should be considered private or public data in a privacy situation. Adequate frameworks should provide some procedure for determining whether certain kinds of practices are vulnerable or not in a privacy situation. Additionally they should help us develop privacy policies to be more protective, trustworthy, and customer friendly.

The idea to add theoretical sensitivity is to begin with the existing theory and "*attempt to uncover how it applies to new and varied situations, as differentiated from those situations to which it was originally applied*" (Strauss and Corbin, 1990, p. 51). Therefore, existing privacy theories and principles are also presented in this section. Nonintrusion, seclusion, control, limitation, and control and restricted access theories are presented and evaluated. Finally, the convenient framework of privacy, the balanced privacy framework, is presented.

2.2.1 Nonintrusion and Seclusion Theory

One view of privacy, originating with Warren and Brandeis (1890), defines privacy as "*being let alone*" or "*being free from intrusion*".

> *'Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls "the right to be let alone" ... the evil of the invasion of privacy by the newspapers ... whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration'*
> *(Warren and Brandeis, 1890).*

A problem with this basic and concrete theory, which Tavani calls *the nonintrusion theory of privacy*, is that it tends to confuse privacy with liberty by suggesting that privacy consists of being let alone. Critics point out that it is possible for one not to be let alone (i.e. be denied liberty) but still have privacy, and for one to be let alone and yet not have privacy. Another view of privacy, which Tavani calls *the seclusion theory*, differentiates privacy from liberty. Its weakness is that it tends to confuse privacy with solitude by tacitly assuming that the more alone one is, the more privacy one has. Critics point out, however, that it is possible for one to have privacy while not necessarily having complete solitude, and for one to have solitude and yet not have privacy (Tavani, 1999b, p. 266).

The two theories considered thus far tend to focus mostly on physical harms to a person that result from either physical intrusion into one's space or interference with one's personal affairs. Considering our arguments for suitable privacy theories, they should focus more on information privacy. Two relatively recent privacy theories, which relate to personal information, are the "*control*" and the "*limitation*" theories.

2.2.2 Control and Limitation Theory

According to *the control theory,*[19] one has privacy if and only if one has control over information about oneself. In a 1975 article, James Rachels lists several cases where "*information about a person might provide someone with a reason for mistreating him in some way"*. Rachels suggests that such cases are misleading when they are taken to indicate why privacy is important. Rachels' main thesis is that we have a need to maintain different types of relationships with different people, and that our notion of privacy is better elucidated by attending to these differences than to instances where

[19] Variations of this privacy theory can be found both in Fried (1970) and Rachels (1975).

information might be used in an abusive way. One proponent of this view, Charles Fried writes, "*Privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves*." (Fried, 1984, p. 209).

One of the most important virtues of control theory in the context of electronic commerce is that the control theory correctly recognizes the aspect of choice that an individual who has privacy enjoys in being able to grant, as well as to deny, individuals access to information about oneself.

Control theory has some weaknesses for the adequate privacy framework. No one is able to have complete control over every piece of information about oneself, although Michelfelder (2001, p. 134) states that "*because the richness of the lived world is not mirrored in the online world, there are fewer relevant privacy values to be concerned about*". But still the control theory has that practical problem. It is highly desirable that we are able to control information about ourselves. However, in a highly networked economy it is simply impossible. We are not able to control vast amounts of electronic information about ourselves. Personally identifiable information about customers "*is well greased and slides rapidly through computer systems around the world, around the clock*." Moor (1997, p. 31).

Another weakness of the control theory is that in focusing almost exclusively on the aspect of control or choice, it tends to confuse privacy with autonomy (Tavani, 1999b). It seems, however, that autonomy in the sense associated with the electronic commerce, as understood as the right to make decisions by oneself that contributes to building meaningful self-identity, tends to slip to the margins in discussions of informational privacy. Michelfelder (2001) states that when we do of think autonomy in conjunction with informational privacy, we are inclined to think of it in terms of having the right to control the access to and the distribution of personal information. However, informational privacy is also a matter of protecting individual autonomy.

The needed amendment to the control theory is a situation dependence, which limits the matters to consider. A relatively new theory offering assistance in this area is called *the limitation theory*[20] by Tavani (1999b). The limitation theory recognizes the importance of setting up zones of privacy. Privacy consists of the condition of having access to information about oneself limited or restricted in a certain situation. One important weakness of the limitation theory is that "*it tends to underestimate the role of control or choice*

[20] The background of the theory, see Gavison (1980).

that is also required in one's having privacy" (Tavani, 1999b, p. 267). Some variations of the limitation theory suggest that a person's privacy correlates with the extent to which information about a person is limited. Therefore privacy according to the limitation theory would seem to be very close related to secrecy. It seems, however, that in some contexts the word '*private*' is virtually synonymous with the word '*secret*'; or '*confidential*'. Thompson (2001, p. 15) points out that when we say '*They want to keep some aspect of their life private in order to avoid embarrassment,*' or '*Medical records should be kept private,',* we can substitute the word *'confidential'* for '*private*' without altering the meaning of statement.

In summary, it would seem that none of the preceding theories, nonintrusion, seclusion, control, or limitation, is strong enough to be an adequate privacy framework. But two of those theories, control and limitation theory, sound rather suitable because they attend closely to the concept of privacy as it relates to personal information. Limitation theory has many good features, but if the theory ignores the fact that someone who has privacy can choose to grant as well as to limit or deny others access to information about oneself, the theory needs some amendments to be adequate for online practices of the Internet. Control theory has that missing feature, but because it does not include the condition of having access to information about oneself limited or restricted in certain situations, its perspective is too wide and open-ended to be practical in the electronic commerce setting.

However, since both the control and limitation theories address privacy issues related to personal information and access to that information, these two would be useful in helping us to better understand those privacy issues related to electronic commerce. Neither control nor limitation theory is adequate in itself since neither theory provides a sufficiently comprehensive account of privacy and the possibility to use that information, so we will focus on the combination of those two theories.

2.2.3 Control and Restricted Access Theory

Moor (1997) presents a theory that covers both the preceding weaknesses; *the control and restricted access theory*. This privacy theory is based on his earlier theory, *restricted access view of privacy* (Moor, 1990, pp. 76-80). It focuses on what we should be considering when developing policies for protecting our privacy; in order to protect ourselves we need to make sure the

right people and only the right people have access to relevant information at the right time.

The control and restricted access theory includes some expansions of the restricted access view of privacy. Basically it has the advantages of the control theory for giving individuals as much control (informed consent) over personal data as realistically possible. But it also incorporates the strength of the limitation theory in maintaining that privacy needs to be understood in terms of situations where access to individuals is limited or restricted. So it recognizes the importance of setting up zones of privacy. Finally it incorporates the strength of both theories in holding that individuals affected by a certain situation need to have some control or choice in determining whether that information will be kept private or not.

The control and restricted access theory provides the opportunity for different people to be authorized for different levels of access to different kinds of information at different times. Moor (1997, p. 31) presents an example that occurs in a modern and computerized hospital. Physicians in the hospital are allowed access to online medical information that secretaries are not. However, physicians are generally not allowed to see all the information about a patient that a hospital possesses. For example, they don't have access to most billing records. In some hospitals, medical information such as psychiatric interviews may be accessible to some physicians and not the others. Rather than regarding privacy as an all or nothing proposition, the control and restricted access theory regards it as a complex situation in which information is authorized to flow to some people some of the time. Ideally, those who need to know have access and others do not.

The control and restricted access theory also helps explain some anomalies about private situations. When we consider privacy, we are generally thinking about situations in which individuals possess damaging personally identifiable information they want to keep others from knowing. Moor (1997, p. 31) points out that "*situations can be private in other circumstances"*. Imagine a situation in a physician's waiting room where scores of customers are waiting for their appointments. A couple begins to argue loudly and eventually shouting to each other about a problem they are having. They go into excruciating detail about various events and catastrophes. Everyone can hear them and many customers feel uncomfortable as they sit there with nothing special going on. Finally, one customer, who thinks he can help, cannot stand it anymore. He asks whether they would like his advice. The couple in unison tells him, "*No, it's a private matter*."

As funny as their comment may be in that situation, it does make sense on several levels. It is not reasonable to claim that an invasion of privacy has occurred, since the couple was the original cause of the information's becoming public[21]. But as Moor (1997, p. 31) writes, "*in private situations the access to information can be blocked in both directions."* The arguing couple did not want to allow information from the customer although they themselves had been rude in revealing details to everyone in the waiting room. Even more ironic is the fact that they are going to see a doctor in order to get advice. Moor (1997, p. 31) states that "*in our culture some activities are required to be done in private*." A discussion of one's intimate health matters may be one of them.

2.2.4 Privacy Principles

McArthur (2001, p. 124) presents two useful principles that emerge from the preceding considerations.
The first principle is:

- *The Mischance Principle*: We cannot reasonably expect to maintain privacy over that which another person could discover, overhear, or come to know without concerted effort on his/her part to obtain this information[22].

Arguing loudly in the waiting room would certainly fall into this category. The mischance principle works, as McArthur (p. 124) points out, "*in a range of possible instances because it is relatively easy to figure out what precautions to take to maintain privacy against casual observation*."

The second principle is:

- *The Voluntary Principle*: If I choose to decrease the relative amount of privacy for myself and information under my control by exposing it to view, I thereby decrease the reasonableness of any expectation that this privacy will be observed.

---

[21] Oliver Sipple (who intervened in an attempted assassination of President Gerald Ford) brought such an action against the San Francisco Chronicle for including in a story that he was gay. He lost the action on the grounds that his sexual orientation was fairly widely known in the Bay Area. Sipple v. Chronicle Publishing Co. 154 Cal App. 3rd 1040 (1984). For a discussion, see Robert L McArthur: Reasonable Expectations of Privacy. Ethics and Information Technology 3: pp. 123-128, 2001 or Rodney A Smolla. Free Speech in an Open Society. Vintage/Random House, New York, pp. 130-132, 1992.

[22] See more about The Mischance Principle (which was originally presented by) Mark Tunik. Practices and Principles. Princeton University Press, Princeton, NJ, pp. 161-190, 1998.

Decreasing the relative amount of privacy is accomplished by increasing the likelihood under the circumstances that the information will come to another's attention through mischance, and therefore our example would certainly also fall into this category. McArthur (p. 125) continues that "*one of the ways in which the voluntary principle is sometimes interpreted is that the failure to attempt to maintain privacy constitutes willingness for that information to become public."* By arguing loudly in the place where people are gathered, the person is *positively* increasing the likelihood of that information becoming known. By arguing loudly in the room where no people are gathered, the person is *negatively* increasing the likelihood that the matter will become known. This principle is later referred to as *the negative voluntary principle*. The extent to which expectations of privacy are reasonable takes into account the social norms governing the particular form of information may have as well as the context. Therefore, the interpretation of whether the person is positively or negatively increasing the likelihood of that information becoming known is not always easy to make.

The Publicity Principle, the Justification of Exceptions Principle, and the Adjustment Principle are presented next. They are also needed to support the implementation of adequate privacy frameworks for privacy practices and policies of electronic commerce. As DeCew (1997, p. 7) states, we should presume in favor of privacy and then develop ways that would "allow the individual to determine for themselves how and when that presumption should be overridden."

Moor's (1997, p. 32) three principles, combined with the mischance and voluntary principles when applied to electronic commerce, enable us to do as DeCew states.

- *The Publicity Principle*: Rules and conditions governing private situations should be clear and known to the persons affected by them.
- *The Justification of Exceptions Principle:* A breach of a private situation is justified if and only if there is a great likelihood that the harm caused by the disclosure will be so much less than the harm prevented that an impartial person would permit breach in this and in morally similar situations.
- *The Adjustment Principle:* If special circumstances justify a change in the parameters of a private situation, then the alteration should become an explicit and public part of the rules and conditions governing the private situations.

The strength of Moor's principles is a very practical one because individuals do not need to have absolute or unlimited control in order to have

privacy on the Internet. The publicity principle entails that we can plan to protect our privacy better if we know where the zones of privacy are and under what conditions and to whom information will be given. Moor (1997, p. 32) states that the publicity principle encourages informed consent and rational decision making, which are important factors in electronic commerce. Once policies are established and known, circumstances sometimes arise which invite us to breach the policy. Moor (1997, p. 32) points out that policy breaches should be avoided as much as possible because they undermine confidence in the policy. However, exceptional circumstances sometimes occur, for example, in the cases related to health issues that are discussed in more detail in Section 3. The adjustment principle normalizes the changed privacy situation. It is an important principle in the setting of electronic commerce where changes of technologies and development of services are pervasive, even paramount. The presented principles and the control and restricted access conception of privacy have the advantage that practices and polices for customer privacy can be fine tuned with consideration to the privacy situation.

2.2.5 Balanced Privacy Framework

In summary, the control and restricted access theory (with the publicity, the justification of exceptions, and the adjustment principle) and the mischance and voluntary principles satisfy all practical needs of the adequate framework of privacy. The negative voluntary principle is particularly promising in sorting out what would constitute reasonable expectations of privacy in many applications of information technology[23]. The control and restricted access theory merged with the principles are called the "*Balanced Privacy Framework*" from this point on.

Considering our arguments for suitable privacy frameworks, the balanced privacy framework focuses on information privacy. This study explores the relationship of Internet electronic commerce, and at the center of this

[23] This point is noted in Justice Harlan's opinion in Katz v. U.S. The Katz case is significant for the development of constitutional protection of privacy against technological intrusion because of Harlan's two-prong test: " first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'." An analysis of the importance of Harlan's test is developed in Richard G. Wilkins. Defining the 'reasonable expectation of privacy'. Vanderbilt Law Review, 40: 1077-1129, October 1987. See also Robert L. McArthur 'Reasonable Expectations of Privacy', Ethics and Information Technology 3: 123-128, 2001.

relationship perspective is the concept of informational privacy. Information practices may conflict with consumers' desires to be shielded from unauthorized use of their personal information. The balanced privacy framework focuses on what we should be considering when developing policies for protecting our privacy in that situation. It does not neglect the important distinction between the different interests affected by electronic commerce. The strength of the balanced privacy framework is its ability to distinguish between the condition of privacy and a right to privacy, and between a loss of privacy and a violation of privacy. It does not downplay the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings. The balanced privacy framework gives individuals as much control (informed consent) over personal data as realistically possible in certain situations. The balanced privacy framework recognizes the aspect of choice that an individual who has privacy enjoys in being able to grant, as well as to deny, individuals access to information oneself. The balanced privacy framework includes the condition of having access to information about oneself limited or restricted in certain situations. One important aspect of the balanced privacy framework is that it results in privacy responsibilities and advantages for both customers and companies.

The balanced privacy framework provides us with a rich framework for deciding whether and how to grant normative protection to certain kinds of personal information currently used in services and activities on electronic commerce. The balanced privacy framework helps us to determine whether certain kinds of personal data should be considered private or public data in privacy situations. Balanced privacy provides a procedure for determining whether a privacy policy statement is vulnerable or not in privacy situations. It is, thus, an adequate framework to use in the content analysis for determining the categories to be used.

2.3 Legislative View of Privacy

2.3.1 Legal Rights

There are two main solutions to deal with legitimate rights of informational privacy. The more common of these is to use the regulatory powers of the

state. The other solution is the voluntary basis. The former is predominant in the EU, which uses very district directives concerning the privacy matter. The latter is very predominant in the U.S., where the greatest likelihood is that industry will be left to develop voluntary guidelines, rather than Congress imposing regulations (Posner, 1992, ch.3).

The notion of privacy has been an evolving concept in the U.S., but privacy was not explicitly mentioned in the Declaration of Independence or in the Constitution of the United States even though portions of these documents implicitly support a notion of privacy as protection from governmental intrusion, particularly the physical invasion of people's houses. In the 1960s and 1970s the legal concept of privacy was expanded to include protection against government interference in personal decisions about contraception and abortion (DeCew, 1997). The constitutional right to privacy was first established by U.S. Supreme Court decision[24]. In this decision, a Connecticut law making it illegal to provide information about contraceptives, including instructions on their use, was found to be unconstitutional. Its moral basis is largely rooted in the value of personal autonomy.

The original concept of privacy has become informationally enriched in the computer age. Its moral basis lies in a host of different values, including personal liberty and dignity, solitude, self-esteem, and self-identity. This shift in emphasis has been brought about because of the development of the computer and its use in collecting large databases of personal information (DeCew, 1997; Moor, 1998). Informational privacy as related to dealing with various kinds of privacy interests and control over personal information is protected by the Fourth Amendment and tort law[25] (DeCew, 1997). Additionally, some other 'special' privacy laws and data protection guidelines have been instituted to protect personal information in the U.S. In particular, some form of normative protection has been explicitly granted to personally identifiable information considered intimate, sensitive, or confidential (Nissenbaum, 1997). This is very much because the database of credit histories or medical records used in normal business provides an ongoing opportunity for misuse and abuse – "*a case in point is the privacy of medical records*." McArthur (2001, p. 127). After many complaints that medical records were being transferred from legitimate users – such as insurance companies – to secondary users – like credit bureaus – the Health Insurance

[24] At 381 US 49 (1965).

[25] "An offbeat example of property right in intangibles is the right of privacy, usually discussed as a branch of tort law, but functionally a brand of property law." (Posner, 1992, p.43).

Portability and Accountability Act (HIPAA) of 1996 was passed by Congress[26]. To date, privacy protection law in the U.S. also includes information obtained from and/or about children (the Children's Online Privacy Protection Act, COPPA[27]) and financial data (the Gramm-Leach-Bliley Act, GLBA[28]).

In summary, there was little legal protection for health information – online or offline – until the release of HIPAA regulation. But while HIPAA regulation is an important step toward boosting the public trust and confidence in the U.S. health care system, its application is limited. Due to constraints on the Department's rulemaking authority, the regulation does not cover a significant portion of the health-related activities that take place online. HIPAA regulation only applies to three health care entities (Choy, Hudson, Pritts and Goldman, 2001, p. 6):

- Health care providers, such as doctors, hospitals and pharmacists, who electronically transmit health claims-related information in standard form;
- Health plans, such as traditional insurers and health maintenance organizations (HMOs); and
- Health care clearinghouses that process health claims information is a uniform format for providers and insurers, such as WebMD Office.

A person or organization that falls within one of these categories is considered to be *a covered entity*. This is a critical factor in determining whether health information is protected under the regulation. It will, however, be difficult for consumers to tell whether any given provider is subject to regulation, since not all health care providers fall under the definition of "*covered entity*". Many health Web sites are not owned or operated by one of these three entities. Therefore, while online health care activities that are already conducted offline by a "*covered*" health care provider or plan will likely be covered by the privacy rule, many other types of health Web sites will fall outside the scope of the rule (Choy, Hudson, Pritts and Goldman, 2001, p. 6). For example, Eli Lilly and Co. (also Global Health Trax and

---

[26] Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. 1320d to d-8 (West Supp.1998). The Department of Health and Human Services finally issued administrative provisions for this bill in late December 2000. See http://aspe.hhs.gov/admnsimp/index.htm or Federal Register, December 28, 2000, for the implementation details (which go into full effect in 2003).

[27] For more information, visit the Federal Trade Commission's COPPA site at http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/adults.htm

[28] It was enacted in 1999 and became effective on July 1, 2001. The GLBA requires financial institutions, including insurance companies, banks and securities firms, to protect the security and confidentiality of non-public personal information for distribution beyond the institution, Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-6809 (2000).

SelectQuote Insurance Services[29]) is not a covered entity so the health information that consumers provide on prozac.com is not protected by the privacy regulation. The key is that the email reminder originates from someone who is not covered by the privacy rule. If, in contrast, a covered physician sent a patient an email reminder, the email would be covered by the privacy rule.

To determine whether a person or organization is a covered provider under the privacy rule, a consumer would need to answer three key questions:

- Is the person or organization a health care provider as defined by the rule?
- Do they transmit health information[30] in connection with one of the financial or administrative "*standard transactions*" listed in HIPAA?
- Do they transmit that information electronically in the required "*standard format*"?

A provider is only covered by the privacy rule if the answer to all of these questions is "yes". Answering even the simplest of these questions, however, may not be as easy as it appears (Choy, Hudson, Pritts and Goldman, 2001, p. 12). The result is that the same activities conducted at different Web sites will be subject to different legal treatment. Specific activities like filling a prescription, receiving email alerts or getting a second opinion may be covered by the new regulation at one site and unregulated at another.

Additionally, even Web sites that are run by covered entities engage in diverse activities, many of which are not covered by HIPAA. Many Web sites provide a variety of services, some of which are not considered "*health care*" functions under the regulation. It is not clear in many cases what activities, even at "*covered*" sites, may fall outside the scope of the regulation. Consumers may engage in online health activities with the expectation that the personal information they provide to a specific health Web site is protected when, in fact, there are no privacy protections afforded by the federal

---

[29] All companies are examples where customers' vulnerabilities have been realized, see Section 1.1.

[30] Only individually identifiable health information that is transmitted or maintained by a covered entity is protected by the regulation (i.e., "protected health information"). This is true regardless of the format of the information – electronic, paper or oral. Individually identifiable health information as defined in the privacy rule as information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that information can be used to identify the individual. Privacy Rule, § 164.501, available at http://www.hhs.gov/ocr/regtext.html

regulation. On these sites, it will be difficult for consumers to know what activities are covered by HIPAA and what activities are not (Choy, Hudson, Pritts and Goldman, 2001, p. 6).

For example, drugstore.com[31] sells both drugs pursuant to a prescription and over-the-counter products. While information related to the prescription drug will be covered by the privacy regulation, information related to the over-the-counter product will not. The privacy rule covers only identifiable information related to "*health care*". This term does not include selling or distributing non-prescription health care items. This scenario could pose serious concerns for some online patients. Consumers often use the Internet to purchase health items in the belief that their purchase will be anonymous (Choy, Hudson, Pritts and Goldman, 2001, p. 14).

Some Web sites will be covered by the regulation, and consumers will benefit from the new privacy protections required of these sites. Under the first-ever federal privacy regulation, consumers have the right to inspect and copy their own health information (a right that previously existed only in about half of the states). Consumers will receive notice about how their personal health information will be used and shared with others and what options they have to restrict disclosures. They will have the right to limit disclosures in many circumstances. Furthermore, the regulation creates a new "*duty of care*" with respect to health information, so in addition to the penalties that can be imposed by the Department of Health and Human Services; it is possible that violations of the regulation may be grounds for state tort actions (Choy, Hudson, Pritts and Goldman, 2001, p. 2).

However, the majority of Americans say that new laws need to be written to protect online privacy. Fully one in four Americans say they don't know what to answer, because they are not sure how the Internet works or how current laws work, or both. Indeed, Internet technologies are new and mysterious to most Americans, and that could be one reason they think older laws might not be appropriately applied to the Internet (Fox, 2001).

2.3.2 Expansion of Legal Rights

While all the discussed regulations are important steps toward protection of sensitive information their applications are limited in the context of electronic

[31] At http://www.drugstore.com

commerce[32]. Thus, legitimate concerns about privacy arise when all kinds of information retrieval, transfer, and manipulation are widely supported by electronic means. This speed and convenience easily lead to the improper exposure of sensitive information. The activity of storing and retrieving information has been enhanced to the extent that all of us now have a legitimate basis for concern about improper use and release of personally identifiable information through the networked economy. Additionally, most non-confidential personal information gathered from an individual's activities, which is called "*spheres other than the intimate*", has no sufficient protection (Nissenbaum, 1998) and it rests mainly on the value judgments of different partners.

In reflecting on what guidelines can best protect online informational privacy (also that which is not intimate) in a commerce-related setting, the US Federal Trade Commission (FTC, 1973) has developed (voluntary) principles of fair information practice (FIPs[33]) for commercial Web sites:

- There must be no personal data record-keeping systems whose very existence is secret;
- There must be a way for a person to find out what information about the person is in a record and how it is used;
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent;
- There must be a way for a person to correct or amend a record of identifiable information about the person; and
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

When those principles are matched against the privacy directives and recommendations of the EU, they appear to be remarkably similar in nature

[32] State laws do not offer adequate protection of information collected by health Web sites either. Protection varies greatly from state to state, and in general only applies to some of the core players in the health care arena (Choy, Hudson, Pritts and Goldman, 2001).

[33] The Code of Fair Information Practices, U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, viii, http://www.epic.org/privacy/consumer/code_fair-info.html, 1973.

(Michelfelder, 2001, p. 132). Approved in 1995 and implemented in 1998, EU Directive 95/46/EC[34] affirms that data-subjects must,

- unambiguously give consent for PII to be gathered online;
- be given notice as to why data is being collected about them;
- be able to correct erroneous data;
- be able to opt out of data collection; and
- be protected from having their data transferred to countries with less stringent privacy protections.

In terms of their content, parallels can be found between the Directive and the principles. The main difference in the Directive is a piece of European legislation that is addressed to Member States. Once such legislation is passed at the European level, each Member States must ensure that it is effectively applied in their legal system and that the Directive prescribes an end result. The 15 Member States of the EU were required to bring their national legislation in line with the provisions of the Directive by October 24, 1998.

2.3.3 Health Care Privacy Policy

The mechanism by which consumers are typically made aware of a U.S. company's privacy practice is through the presence of a privacy policy. Privacy policy statements interact to produce and sustain an online presentation of the company and produce a convincing performance, which is discussed in this section.

The finding of Choy, Hudson, Pritts and Goldman study (2001, p. 4) is that a significant portion of activities at health-related Web sites are not covered by HIPAA and, therefore, a Web site privacy policy is an important document to reflect practices of the online health organization. A privacy policy comprehensively describes a Web site's information practices and is located in an easily accessible position on the site. A privacy policy describes the kinds of information collected by the Web site and the way that information is handled, stored, and used. Every organization involved in electronic commerce transactions has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. A privacy policy should directly reflect an organization's privacy rules and practices no

[34] DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

matter what business function uses the information. Any organization embarking upon online transactions should be prepared to address privacy matters in advance, clearly, openly and accurately. Organizations must also consider other organizations with which they interact, and take steps that foster the adoption and implementation of effective online privacy policies by those organizations as well (FTC, 1998; FTC, 2000).

Privacy policies and privacy practices reflect the ethical views of an organization, and therefore provide an indication of perceived trustworthiness to those who conduct business with a given organization. Consumers will be less likely to patronize stores that fail to create a sense of trustworthiness. Creating and maintaining a successful business requires trust, "*a trustor's expectations about the motives and behaviours of a trustee*" (Doney and Cannon, 1997, p. 37), and an effective privacy policy is one means to increase trust between a consumer and an organization. Internet users are concerned about threats to their privacy while online. Trust is associated with a lower perceived risk of visiting at the site, and we expect trust to be affected by the consumer's perceptions of a Web site privacy policy. Several studies have shown that Internet users are more inclined to trust a Web site if it simply posts a privacy policy (Earp and Baumer, 2003; Goldman, Hudson and Smith, 2000).

Although there are clearly many other factors beyond the presence or absence of a policy statement that influence the decision to do business (Ellinger, Lynch, Andzulis and Smith, 2003, p. 215), prospective customers may take a company's failure to articulate a privacy policy on its Web site as an indication that a Web site is not a trustworthy. In an Internet context, customers rarely deal directly with any person and therefore customers depend on an impersonal electronic storefront to act on their behalf (Culnan and Armstrong, 1998). Internet companies which provide an unclear, conflicting, and overly concise privacy policy should be considered suspect. The worst situation is that there is no privacy policy statement available at all. Web sites should be set up to encourage business, not to preclude it. If prospective customers cannot easily find what they are looking for on a health care Web site, they may move on to find another site that makes its informational and interactive content more apparent. In addition, Internet privacy policies are critical due to the increase in information collection for various business functions, as evidenced by the increased attention received by companies whose privacy practices are called into question (e.g. FTC, 2000). The Federal Trade Commission recommends that these policies should focus on practices of the Fair Information Practices (FTC, 1998; FTC, 2000).

When the Fair Information Practice Principles are applied to an online environment, *the principle of notice* requires that commercial Web sites not only let their visitors know what personal information is being collected about them but also how this information is collected, whether or not it is distributed to third parties, and whether or not other parties are permitted to gather information at these sites. When it is adequate, *the principle of choice* involves letting online customers decide if the information they knowingly provide to a Web site for a particular purpose can then be used by that Web site for other reasons. *The principle of access* gives customers the ability to examine the data collected about them by a particular site and make corrections if necessary, while *the principle of security* means that Web sites need to protect the personal identifiable information they collect from falling into the hands of unauthorized others (Michelfelder, 2001, p. 131).

A 1999 study of twenty-one leading health-related Web sites had found that the policies and practices of many of the sites did not meet minimum fair information practices (Goldman, Hudson and Smith, 2000). For example, third parties may collect personally identifiable information through banner advertisements without host sites disclosing this practice to the user. Following the release of the report, several members of Congress requested the FTC to immediately initiate an investigation of whether certain health Web sites may be engaged in "*unfair or deceptive acts or practices*" (Pitofsky, 2000a; Pitofsky, 2000b). The commission maintained that industry self-regulation had fallen short. Even as it agreed to a self-regulation scheme with Internet advertisers, the FTC called on Congress to expand the agency's enforcement power "*to ensure adequate protection of consumer privacy online.*" (Pitofsky, 2000a, 2000b). A subsequent Federal Trade Commission (FTC, 2000) investigation of several of these health Web sites found that the sites made changes to their policies in response to the findings of the report.

Internet customers may not know all the tricks when it comes to protecting their privacy online, but they do know problems when they see them. If their trust is betrayed, they want vengeance. Companies should keep their promises – or else Internet customers want to punish companies and executives when they violate customers' privacy. If an Internet company violated its stated privacy policy and used personal information in ways that it said it wouldn't, over 90% percent of Internet users want privacy violators to be disciplined (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 3).

There is no law requiring any Internet service to display a privacy policy. The Progress and Freedom Foundation (PFF) surveyed a random sample of highly-visited Web sites and found that over 80 percent of those Web sites

posted a privacy policy (Adkinson, Eisenach, and Lenard, 2002), showing a significant increase from the 1990s, when only 14 percent provided any notice regarding information privacy practices (FTC, 1998). There seems, anyhow, to still be differences among business segments, for example, according to the recent study by Ellinger, Lynch, Andzulis, and Smith (2003, p. 206), only one in five of the carrier Web sites explicitly displayed privacy policies. Health Web sites are more likely than non-health related sites to post privacy policies, and many health Web sites do have privacy policies (Goldman, Hudson and Smith, 2000). According to this study it seems that most health care Internet services in the U.S. display a privacy policy that describes the site's privacy-related information practices.

2.4 Conclusion

It seems that privacy is a broad and, in many ways, elusive concept. Privacy is, however, grounded instrumentally and intrinsically – instrumentally, as support for the core values, and intrinsically, as an expression of security and more. Thus, there is a presumption throughout this study that privacy is a positive value that is worth protecting, and that federal health privacy regulation does not provide adequate support for it. The mechanism by which consumers are typically made aware of a U.S. company's privacy practice is through the presence of privacy policy.

The extent to which the new federal health privacy regulation will impact on e-Health will depend largely on whether or not a Web site or Internet service is affiliated with or controlled by a covered entity, and whether that site or service collects identifiable health information. Web sites not associated with a provider, plan, or clearinghouse and not acting on behalf of these entities will fall outside the scope of regulation. Personal health information collected and maintained by these Web sites will, therefore, be left unprotected by the federal regulation. Given the wide range of activities on the Internet and the relatively narrow scope of the regulation, it is likely that a great deal of health information collected on health Web sites will not be covered by the new regulation.

Additionally the situations that are normatively private can vary significantly from culture to culture, situation to situation, and time to time. This does not mean that the privacy standards are arbitrary or unjustified; they are just different. A safe retreat to a realm of pure facts where everything is black or white, true or false, law statutes or voluntary basis, without any

consideration of values is never possible, and that also includes privacy practices and policies. Some privacy values could be more important than others, but there is no such thing as a greatest good. Some people will emphasize some values and aspects more than others.

Core human values are articulated in a multitude of ways, but they also constrain the realm of possibilities. To say that we share core values is a first step in the argument toward grounding ethical judgments. If we respect the core values of everyone, then we have standards with which to evaluate actions and policies. The core values provide a framework for analysis in privacy policy. They provide us with a set of standards with which to assess policies, even in situations where no previous policies exist, and with which to assess other value frameworks when disagreements occur. By using the core value framework, some privacy policies can be judged to be better than others.

To determine whether the privacy practice or policy of a Web site actually violates the privacy of customers, an adequate privacy framework, the balanced privacy framework, is determined. The strength of the balanced privacy framework is that it does not neglect the important distinction among the different interests affected by electronic commerce. The balanced privacy framework focuses on both customers and companies. Rules and conditions governing a private situation should be clear and known to the persons affected by them. It also underlines the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings. The framework provides us with a rich scheme for deciding whether and how to grant normative protection to certain kinds of personal information currently used services and activities on the Internet. It would help us to determine what is required to have privacy in electronic commerce. The balanced privacy framework encourages informed consent and rational decision-making, which are important factors in electronic commerce. It is because the balanced privacy framework has the advantage that practices and polices for customer privacy can be fine-tuned with consideration to the privacy situation.

3 NETWORKED HEALTH ECONOMY

"The Best Prescription is Knowledge"™
Dr. C. Everett Koop[35]

The Internet offers consumers unprecedented access to a wide range of health care goods and services. This giant network of networks has become a major catalyst for both electronic commerce and electronic business and it is being taken into usage in the health care segment at an increasing pace. The Internet has the ability to link health organizations inside and outside of the company into a single network, creating the foundation for a vast electronic health service.

Since HIPAA's passage in 1996, there has been an explosion of health-related activity on the Internet. In 2000, over 17,000 different health care Web sites offered a wide range of products and services on the Internet (Goldman, Hudson, and Smith, 2000). In 2001, with an estimated 100,000 health related Web sites, the Internet has changed the way that Americans access health information (Eng, 2001; Eysenbach and Kohler, 2002). Health Web sites are proving popular. A few are ranked in the top 500 most visited Web sites by Media Metrix, a service provided by Jupiter Media Metrix, which measures user activity and site traffic. In the past two years, it is estimated that the number of people accessing health information online has doubled (Choy, Hudson, Pritts and Goldman, 2001, p. 4). But it is suggested that much more is still to come. Customers want more information on drug interactions, diagnostic tools or symptom finders, electronic medical records and test results, more ways to connect with local resources, and a doctor-patient email (Fox and Fallows, 2003, p. 29). Additionally, health customers are disappointed by the lack of access to their doctor's calendars – they would like to make appointments online (Sciamanna, Clark, Houston, and Diaz, 2003).

The Internet is an effective tool for receiving and sharing data and, thus the Internet has a range of capabilities that health providers are using to exchange information internally or to communicate externally with other organizations. Business functions on the Internet are, however, relatively new, resulting in modifications to how some organizations conduct business. Thus, along with bringing many new benefits and opportunities, the Internet has created a new set of management challenges. Changes in organizational objectives, business

[35] At http://www.drkoop.com

protocols, organizational focus, and management are some reasons why the practices and policies of an organization might alter.

This section discusses how enriched health information is processed and what kinds of vulnerabilities might result. It also presents possible scenarios, and finally introduces the Balanced Privacy Model.

3.1 Privacy Situation of Health Care

The last five decades have seen dramatic changes in the technical and organizational configurations of information system. During the 1950s, organizations were dependent on computers for a few critical functions. The 1960s witnessed the development of large centralized machines. By the late 1970s and the 1980s, information architecture became complex, and information systems included telecommunications links to distribute information. During the 1990s, information architecture was an enterprise-wide information utility, which in turn was connected to vendors and customers through the information and communication technology (ICT). Pearson (2003) suggests that the information and communication technology explosion continues and actually, it's accelerating. She has presented information technology trends as follows:

- Chips per dollar – a 10 times increase in 5 years;
- Computing power per dollar – a 10 times increase in 4 years;
- Storage per dollar – a 10 times increase in 6 years;
- Communication backbone – a 100 times increase in 5 years; and
- Communication local loop – a 100 times increase in 5 years.

More inexpensive and more effective information technology has opened up many exciting possibilities for organizing and running a business and are transforming organizations and the use of information systems in everyday life. Today's global economy offers consumers unprecedented access to a wide range of goods and services. Increasingly, the Internet is providing the underlying technology for these changes. It is creating a universal platform for buying and selling goods and for driving important business processes inside the firm. The Internet has become an important element of doing business.

Although it is difficult to pinpoint when the Internet began to create expectations among all Americans about the availability of online health care information, two snapshots taken from the past couple of years are enlightening. During a study of community technology initiatives in Cleveland

in late 2000, Pew Internet project researchers found that some low-income people who come to the community center to pick up Internet skills were driven in part by the aggressive marketing campaigns of major Internet service providers. They wanted to know about the CD-ROMs they were receiving in the mail and what the Internet was all about. But these nascent users had a very thin knowledge base. Fast forward to two years later in another community technology center in Virginia, and Pew Internet researchers found that very new Internet users quickly embraced the Internet for sophisticated applications such as filling medicine prescriptions online (Horrigan and Rainie, 2002, p. 5).

Customers and health providers can complete health-related transactions, regardless of their location. A vast array of health goods and services are being advertised, bought, and exchanged worldwide using the Internet as a global marketplace. There is abundant evidence that use of the Internet has played a role in revolutionizing the more than USD 1 trillion health care industry in America. Doctors, hospitals, health maintenance organizations (HMOs), insurance companies, and Internet firms are using the Internet to retool the business of medicine. In addition, more and more health providers are interacting with their colleagues via email and are interested in using email and the Web to interact with customers (Mold, Cacy and Barton, 1998) to locate the most current literature on the effectiveness of specific treatments, and to conduct research themselves, sometimes in collaboration with colleagues on the other side of the world (Fox and Rainie, 2000, p. 8).

Online business can create new market niches via the Internet. A health provider can provide a specialized product or service that serves a narrow target market better than existing competitors and discourages potential new competitors. For those reasons, the health provider must acquire and use information and knowledge[36] about the online customers, services, and service processes. In an era characterized by rapid change and uncertainty, it is claimed that successful companies are those that create new knowledge and disseminate it through the organization (Nonaka, 1991). "*Knowledge today is a necessary and sustainable source of competitive advantage." (*Earl and Scott, 1999, p. 29). Knowledge is displacing capital and labor as the basic

[36] "Knowledge is commonly distinguished from data and information. Data represent observations or facts out of context that are, therefore, not directly meaningful. Information results from placing data within some meaningful context, often in the form of a message. Knowledge is that which we come to believe and value on the basis of the meaningfully organized accumulation of information (messages) through experience, communication, or interference." Michael H. Zack (1999). "Managing Codified Knowledge", Sloan Management Review, Summer 1999.

economic resource (Drucker, 1995). It is widely stressed that a corporation's competitive advantage flows from its unique knowledge and how it manages that knowledge. That observation rings increasingly true as we enter the complexity of the global electronic economy (El Sawy, Eriksson, Raven, and Carlsson, 1999).

Online companies can use very large pools of data from multiple sources to rapidly identify "*good customers*" or "*prospective customers*" and suggest individual responses. For example, Amazon.com[37] describes the perfect online shopping experience as a customer launching their browser and finding on the screen the exact item they want – which the customer may not have even known about until that very moment. Embedded in the cookie is an identifying number that alerts a server to the customer's presence. Using this cyber fingerprint, the online company is able to monitor where the customer goes on the Internet, what he clicks on, what he buys, and what he does not buy. This monitoring reflects the customer's online behaviors and helps marketers target ads especially for that customer. It is possible to transform raw data about a customer's online behavior into useful information and knowledge which can then be used by the online company for future applications, exchanged with other online companies, or sold to businesses that operate in the physical realm. Raw data can be merged into "*data pool*" – systems. This system can be "*mined*" more widely by the online organization. These kinds of information systems enable companies to finely analyze customer buying patterns, tastes, and preferences so that they can efficiently pitch advertising and marketing campaigns to smaller and smaller target markets. Additionally, the Internet opens up the possibility of mining large pools of data by using small desktop machines remotely, permitting an invasion of privacy on a scale and precision that was previously unimaginable. Through special communication and technology standards, any computer can communicate with virtually any other computer linked to the Internet.

3.1.1 Informationally Enriched Health Process

The introduction of the Internet is accompanied by a synchronized development of the business activities. It forms the basis for information exchange among organizations and its business partners as well. The conceptual framework for such development comes from the discourse of

[37] http://www.amazon.com

business processes (Hammer and Champy, 1993). The concept of business process has been fostered in an environment close to Porter's value chain (Porter, 1985; Porter and Millar, 1995). Additionally, the value chains constitute larger value networks or systems in the following way:

> *"An organization's value chain as a part of a value system is composed of the value chains of a company, its suppliers, its distributors and its customers. By paying attention to the inter-company linkages in the value system a company can add value not only to itself butalso to those in the value system"*
> *(Porter and Millar, 1995).*

The low cost of electronic networks makes it valuable to communicate with health partners and customers electronically. Handling transactions electronically reduces transaction costs and delivery time for some goods, especially those that are purely in digital form. Business partners can directly communicate with each other at a very low cost, bypassing middlemen and inefficient multilayered procedures and, thus, the Internet implements many advantages in the value chain of the company. The Internet has created a networked economy, where communication and transactions often take place almost immediately and can involve many interactions (Whinston, Stahl, and Choi, 1997).

The possibilities of the Internet have been observed in many sectors, including health care. Companies can no longer expect the health services and health practices that made them successful in the past to keep them competitive in the future. The Internet presents many challenging opportunities for health care-related businesses. As a result of the information and communication needs of both health care providers and customers, many companies and health care organizations in the U.S. have decided to implement different kinds of information technology to support information searching, acquisition, and transfer. Health care providers have been starting to use Internet systems to create products and services that are tailored to meet the precise specifications of individual customers (Goldman, Hudson, and Smith, 2000; Eng, 2001; Eysenbach and Kohler, 2002; Choy, Hudson, Pritts and Goldman, 2001; Fox and Fallows, 2003; Sciamanna, Clark, Houston, and Diaz, 2003).

Web sites are available to consumers and business partners 24 hours a day. In 2000, customers reported that one of the most important aspects of an online health Web site is the fact that it is available at any hour of the day or night, from wherever they are able to log on (Fox and Fallows, 2003, p. 33). A wide range of health care activities and services, from general health

information to online support groups and personal health management tools, are offered online. Consumers can "*surf*" the Web for information about symptoms, remedies and health insurance rates.

In a survey of Internet consumers who go online for health care information, the Pew Internet & American Life Project found the following (Fox and Rainie, 2002):

- Almost every customer has looked for information about a particular illness or condition at one time or another.
- Two-thirds of all customers have looked for information about prescription drugs.
- More than half of all customers have gathered information before visiting a doctor.
- Nearly half of all customers have looked for alternative or experimental treatments or medicines.
- A typical customer searches for medical information only occasionally, and she relies on search engines and multiple sites.
- More than half of customers do health searches every few months or even less frequently.
- A typical customer visits several sites during a typical search and does not have a favorite site.
- Worrying about someone else's health issue is the main motivation for customers to go online for medical advice, whether for a friend, spouse, child, or parent. Eighty-one percent of customers have gone online because someone they know was diagnosed with a medical condition.
- Even without any outside help, a typical customer feels it is quite easy to get the information she needs.

Fox and Fallows (2003, p. 15) found a correlation between visits to health care providers and researching health issues on the Internet. People who visit a doctor or clinic are more likely to have gone online for health information, and vice versa. This suggests that when people are sick or have health issues rise to the fore, they turn to both their traditional practice of visiting a health care provider and the newer resource of searching the Internet for health information.

In the summer of 2001, about 45 million Americans said the Internet has improved the way they take care of their health, compared with 25 million Americans who said the same in August 2000 (Fox and Rainie, 2002). Previous reports indicate that patients feel that information on the Internet is "*better than*" information from their doctor (Ferguson, 2002). In fact, patients

with lower self-rated health (i.e. sicker patients) are the most likely to talk to health care providers about the information they found on the Internet (Houston and Allison, 2002). This revolution in health care information has great potential to affect the way that customers interact with their physicians. Other researchers found that when a patient brings online health information to an appointment, the doctor spends about ten extra minutes discussing it with them. Oncologists also reported that use of the Internet had the ability to simultaneously make customers more hopeful, confused, anxious, and knowledgeable (Heft, Hlubocky and Daugherty, 2003).

KPMG's Internet Maturity Model (presented in Ellingher, Lynch, Andzulis and Smith, 2003, p. 200) suggests that Web sites go through four distinct stages as the company's electronic commerce strategy evolves – marketing, publishing, transactional, and interactive.

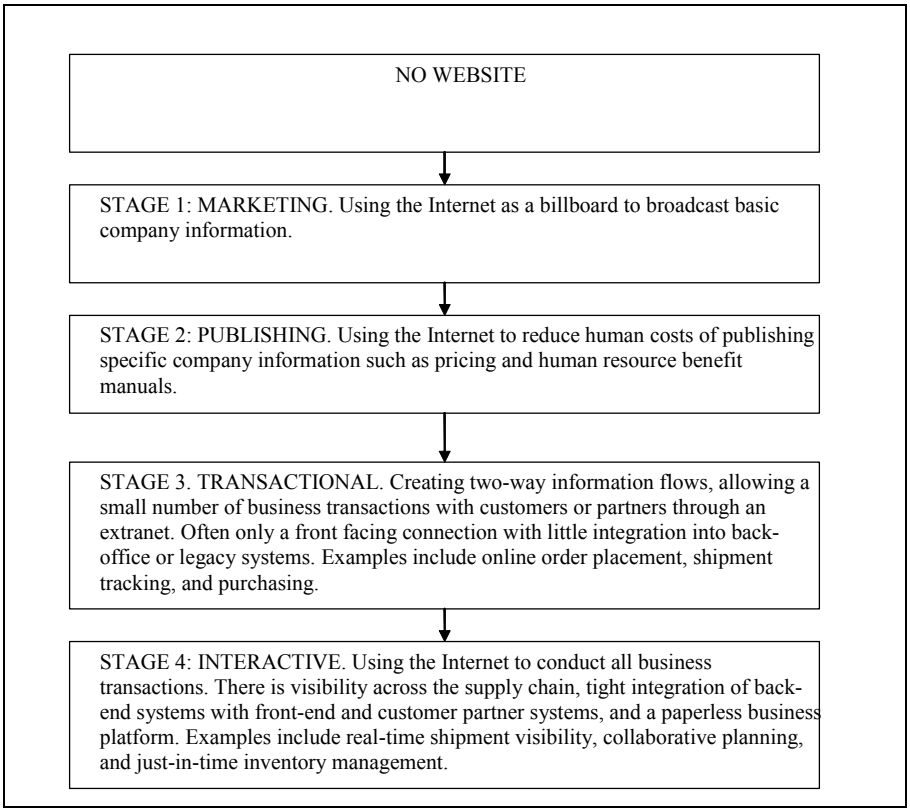

Figure 2: KPMG's Internet Maturity Model.

According to KPMG's Internet Maturity Model, the Internet provides the *transactional* and *interactive stages* when the health provider's electronic

commerce strategy evolves. But even in a situation where Internet Web pages are used only for marketing or publishing reasons, the Internet has an effect on customers' buying behavior. If a store provides only product information online, but does not sell products on its Web site, it has an impact on customer buying habits. About half of Americans said a Web site – even one that did not permit online purchasing – would make it more likely that they would go to the actual store to buy the product. In other words, having a Web site helps a business even if the site does not enable transactions (Horrigan and Rainie, 2002, p. 14). But the multimedia capabilities of the Internet can be used to create new health products and health services and closer relationships with customers. Activities currently available on many health care Web sites include: purchasing, provision of clinical information, professional interaction, and personal health records.

Until recently, most health care information was in paper records. While a paper-based system has vulnerabilities, it also places some natural limits on the ability of information collectors to share and disseminate information. They offer some protection from improper dissemination when the information is being shared for legitimate, health care-related purposes. The difficulties and expense of transmitting health information in a paper-based system have motivated the health care industry to migrate toward electronic collection, storage, and transmission of information, such as via the Internet. Health data can be easily located, collated, and organized. With the click of a mouse, sensitive and personal information can be sent to any number of places thousands of miles away (Choy, Hudson, Pritts and Goldman, 2001). Furthermore, the pace of e-Health development has meant that more and more traditionally offline health-related activities can now be done online.

Transactional and *interactive* online systems will have many impacts on organizations. Additionally, organizations in different circumstances will experience different effects from the same technology. The changes in information technology potentially change an organization's structure, culture, politics, and work. Considering the mutually adjusting relationship between technology and the organization, there are several ways to visualize organizational changes. Implementing information systems has consequences for task arrangements, structures, and people. Leavitt used a diamond shape to illustrate the interrelated and mutually adjusting character of technology and organization (Figure 3).

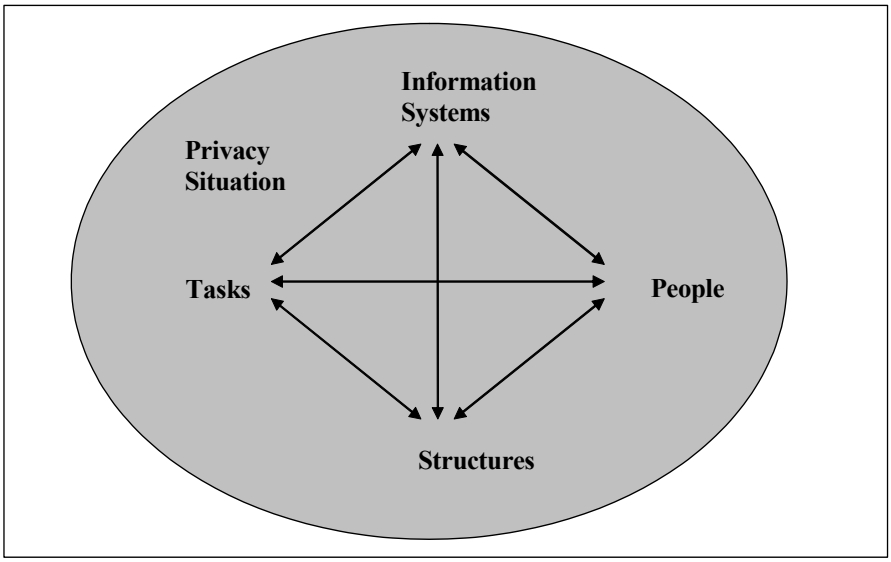

Figure 3: Leavitt's model (1965).

According to Leavitt's model (1965), all four components must be changed simultaneously in order to implement change[38]. Leavitt's model can be associated with the distinction between plans and situated action (Suchman, 1987). Not all (health) service processes can be described in detail for practical (the huge number) and conceptual (unpredictable variations) reasons. In situated action, the actor acts intentionally and competently without a ready-made plan; letting the awareness, interpretation, experience and overall goals to have an implicit impact. Such activity can be said to be locally (in place and time) articulated (Strauss, Fagerhaugh, Suczek and Wiener, 1985, p. 151; Star, 1991).

Industrial production is often based on standardization of the products and working practices of standard operating procedures (SOPs). Anselm Strauss (1988) stated that many elements of industrial production are almost fully rationalized and articulation work is built in as part of this rationalization. All of that can be done because goals are clear, and the evaluation of results throughout the course of work is both possible and feasible. Service, on the other hand, is personal and mainly intangible. Service is typically a unique act, transaction, or process that does not easily lend itself to standardization. In respect to time, it is typical that the production, distribution and consumption

[38] The changes also reflect on the privacy situation, and therefore the author has added the privacy situation to Leavitt's original model in Figure 3.

take place simultaneously. Networking has recently made it possible to transcend this restriction to some extent, but the basic setting of services is still constituted by this kind of simultaneity and joint location of provider and customer (Nurminen and Järvinen, 2001).

When information systems are added to the scheme of situated action or articulation work, privacy issues are more challenging. "*When information is computerized, it is greased to slide easily and quickly to many ports of call."* (Moor, 1997, p. 27). While the Internet can be a powerful tool in the delivery of health care, it enables the collection and distribution of highly sensitive information in new ways by online services. It can also leave such information vulnerable to security breaches.

The author has used the term "*Computer Supported Health Process*" (CSHP) but also the term "*Computer Supported Cooperative Health Process*" (CSCHP) in Figure 4, which describes an interaction of various types of health activities in the health care process (Järvinen, 1999, pp. 81-82). Some possible stakeholders are easily mentioned, hospitals, health maintenance organizations (HMOs), insurance companies, doctors, drugstores, and so on. Some of those are considered to be a covered entity.

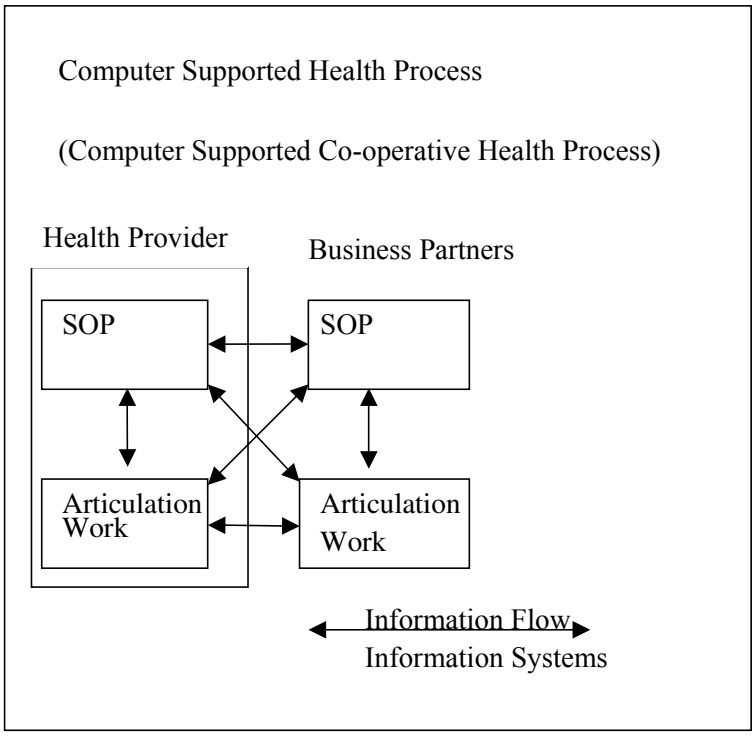

Figure 4: Informationally Enriched Health Process: Standard Operating Process, Articulation Work, and Information Systems.

There are different kinds of activities within or outside information systems, and each plays its part in the total arc of work, either separately or collaboratively. There is a bunch of informationally enriched standard operating procedures, articulation work, and situated actions. Considering Leavitt's Diamond, situated actions without plans and the unpredictable nature of articulation work, there are many potential privacy threats in those sequences of activities. Since more people are involved in the health process, each person may be involved with sensitive information. All those issues reflect in the consideration of privacy situation.

The Internet allows for online communication, and the collection, storage, and transfer of customer health information. The Internet makes information retrieval, transfer, and manipulation quick and convenient. "*Once data is entered into a database it can be stored, searched, and accessed in extraordinarily easy ways that paper files cannot be – at least in practical amounts of time*." (Moor, 1998, p. 16). The activity of service process done extensively by information systems is informationally enriched. The end

result is that the Web site owner – and possibly third parties – has a great deal of health-related information that can be attached to a particular customer without the customer's knowledge or consent. The vulnerability of an Internet customer is significant because information about customers is computerized, and hence easy to transfer, and it is possible for third parties, who may find their own uses for that information, to gather information and send it along networks rapidly.

Because only health providers that fit within the definition of a "*covered entity*" have to comply with the privacy regulation HIPAA, specific activities may be covered by the new regulation at one site and unregulated at another. Additionally, only some information in the health care process is protected health information. The result is that the same transactional and interactive activities conducted at different Web sites will be subject to different legal treatment.

Health plans and providers routinely hire other companies and consultants to perform a wide variety of functions for them, such as legal, financial, and administrative services.[39] They may receive health information on behalf of or from a covered entity. In general, they are not directly covered by the privacy regulation. To ensure that privacy protections follow the information flow, the privacy rule requires that covered entities enter into contracts with business partners that require the recipients of health information not to use or disclose the information other than as permitted or required by the contract or as required by law, and to implement appropriate safeguards to prevent inappropriate uses and disclosures. The regulation establishes specific conditions concerning when and how covered entities may share information with business associates.[40] However, the business associate is not directly subject to the privacy rule. Rather, it is the covered entity that is liable for violations of the contract, and then only if it had actual knowledge of the breach yet did nothing to remedy it. While health care clearinghouses are directly covered by the privacy regulation, in many cases they will be acting on behalf of a provider or insurer, and would therefore be considered business associates of that provider or insurers as well. However, they will be directly liable for violations of the business associate contract and thus violations of the regulation (Choy, Hudson, Pritts and Goldman, 2001, p. 10).

Transactional and interactive online systems will have many direct impacts on customer health service. In fact, electronic health information on the

[39] The privacy rule refers to these as "business associates".

[40] Privacy rule, § 164.504(e)(2), available at http://www.hhs.gov/ocr/regtext.html

Internet can be easily accessible to many different people, including the customer herself. The electronic medium facilitates communication between customers and health providers. A health provider's ability to quickly access a patient's entire medical record, assembled from various sources, can facilitate diagnosis and eliminate medical errors, such as prescribing incompatible medications. Customers can also interact with doctors and other users in chat rooms and by email. They can obtain health care services, such as second opinions and medical consultations, and products, such as prescriptions drugs, online (Choy, Hudson, Pritts and Goldman, 2001).

The medical establishment is beginning to recognize both the potential benefits and pitfalls of using electronic communications in health care. The few doctors and clinics that are already using email recognize that email communications represent more than a shift in a technology; establishing email use can entail wholesale change in office attitudes and practices, not to mention a serious look at the medical and legal ramifications (Fox and Fallows, 2003, p. 19). What are the implications of email correspondence in malpractice suits; what if health-related emails go astray or end up in the wrong hands?

3.1.2 Trust

> *"Most of the time, ..., the Net is neutral. It neither creates social bonds nor destroys them. It does not build trust nor destroy it." (Uslaner, 2000, p. 20).*

This section explores the Internet business from the customer perspective. At the center of this perspective is the concept of trust. Sharing personal medical and health information across the Internet requires a certain leap of faith – or at least a strong sense of privacy and trust (Fox and Fallows, 2003, p. 14). Trust is a critical factor in any relationship in which the consumer does not have direct control over the actions of online company, the decision is important, and the environment is uncertain (Mayer, Davis, and Schoorman, 1995).

Efficiency is one of reasons why people like to use the Internet, and privacy and security issues are cited as the top reasons why more people do not use services online or complete the transactions they start (Luo, 2002). Once the Web site starts asking for personal information, it is likely that many people are put off. They don't know what will be done with their information and

thus they fear it may risk their privacy. A 1999 survey revealed that almost 90 percent of Internet users are concerned about threats to their privacy when online (Cranor, Reagle and Ackerman, 1999).

While the Internet offers unique advantages to both customers and the health care industry, some customers are afraid to take advantage of the benefits because of privacy and confidentiality concerns. The effect of possible opportunism and trust might be dependent on what the consumer is going to do on the Web site, because more than three in four are concerned about Web sites sharing information without their permission, and this impacts on their willingness to use the Internet for health-related activities (Choy, Hudson, Pritts and Goldman, 2001, p. 4). In a November 2000 survey, only 10 percent of customers said that they had purchased medicine or vitamins online. As with other aspects of online shopping, there are more browsers than buyers. For example, customers say that overt commercialism is one reason they have turned away from a Health Web site. Other reasons for turning away were no visible "*seal of approval*" or sloppy or unprofessional design. Part of the reason is that many people prefer to make their actual purchase in stores. Others are worried about the security of their credit card information (Fox and Rainie, 2002).

The Internet is claimed to reduce the advantages of scale of large companies, to lower the costs of entering international consumer markets, and perhaps to reduce the strength of established companies by allowing new merchants to enter and leave quickly. But "*these speculations appear to overlook the importance of the relationship between the consumer and the merchant in this new form of direct marketing."* (Jarvenpaa et al., 2000, p. 45). While it seems at least a bit curious that people will do business on the Internet even as they worry about its security, it doesn't take much imagination to think what type of scare might drive people away from electronic commerce, or perhaps web sites in general. It is suggested that people who already mistrust others will be particularly concerned about Internet security and privacy and "*since most Americans don't trust each other, this is a potentially worrisome feature for the growth of on-line business and investing*." (Uslaner, 2000, p. 18).

The customers who use services in "*the real world*" have the opportunity to develop a relationship with the organization face-to-face. The customers understand that over time the organization knows things about them and they know things about the organization. If the service is transferred to the Internet, sensitivity to privacy is much higher (Sheenan and Gleason, 2001). In the case of Internet services, the contact person is absent from or peripheral to the

service process (Lohse and Spiller, 1998), and then the primary target of the consumer's trust is the organization itself (Chow and Holden, 1997). Customers rarely deal directly with any person and thus this belief may be more difficult for an online company to engender than it is for a conventional merchant.

In a virtual world, the issue of trust is magnified, because "*trust is a critical factor in stimulating purchases over the Internet."* (Quelch and Klein, 1996, p. 70). The substantive long-term issue is, therefore, "*How do customers know whom to trust*?"

Trust is a broad concept, whose values underlie the way that economies and societies function. Trust can be described as the firm belief in the reliability, honesty, and veracity of a person or thing. Concepts of trust overlap with loyalty, which has elements of allegiance and continuing faith in persons or things as opposed to the initial, recognition, and element associated with trust. Trust is one of the major contributors to building social cohesion. "*Trust in other people is trust in strangers, people who are different from yourself ..., trust reflects an optimistic world view and a belief that others share your fundamental values*." (Uslaner, 2000, p. 6). Trust is a governance mechanism in exchange relationships that are characterized by uncertainty, vulnerability, and dependence (Bradach and Eccles, 1989). Trust is interwoven with risk (McAllister, 1995), and both are based on perceptions (Hawes, Mast, and Swan, 1989). The strongest forms of trust are generally evoked by repeated personal interactions by the exchange parties (Doney and Cannon, 1997).

The importance of privacy, confidentiality, and trust are recognized on the Internet, and they are institutional factors that enable Internet transactions to take place. This importance relates not only to Internet transactions themselves, but also reflects the broader concepts of individuals' needs for respect of their privacy and for their protection against opportunism[41]. This is a particularly relevant matter for the Internet, where the traditional trust mechanisms of small groups have been replaced by distance relationships and globalization, and thus sensitivity to the issue of privacy is much higher than before (Sheenan and Gleason, 2001). "*Developmentally, a relationship among parties who have had not prior association is expected to emerge incrementally and to begin with small actions that initially require little reliance on trust*." (Jarvenpaa et al., 2000, p. 46). If the actions are reciprocated, trust tends to spiral upward. If they are not reciprocated, trust

[41] Williamson (1975, p.6) defines opportunism as "self-interest with guile". It includes such behaviors as distorting information and failing to fulfill promises and obligations (John, 1984).

spirals downward (Sitkin and Roth, 1993). One of the consequences of trust is that it reduces the consumer's perception of risk associated with opportunistic behavior by the organization (Ganesan, 1994). Risk perception refers to the "*trustor's belief about likelihoods of gains and losses outside of considerations that involve the relationships with the particular trustee*" (Mayer, Davis, and Schoorman, 1995, p. 726).

In traditional marketing channels, a customer uses size as a signal that an organization can be trusted. The perception of large organizational size implies that other buyers trust the organization and conduct business successfully with it. This experience of others is taken as a reason to trust that an organization will deliver on its promises (Doney and Cannon, 1997). Large size also signals that the organization should have the necessary expertise and resources for support systems such as customer and technical services, and the existence of these issues encourages trust (Chow and Holden, 1997). Reputation, like size, is conceptualized as the consumer's perception of an organization's reputation, where "*reputation*" is defined as the extent to which customers believe an organization is honest and concerned about its customer (Doney and Cannon, 1997). Smith and Barclay (1997) state that a good reputation signals past forbearance from opportunism. The costs of untrustworthy behavior are perceived to be higher for organizations that already have a good reputation. Organizations with strong trademarks are very good examples of business institutions which reflect trust. We have more trust in an organization that is previous known at least by name. The institutions of trademarks and brands reflect an organization's perceived trustworthiness to those with whom it conducts business[42]. Organizations with a good reputation are perceived as being reluctant to jeopardize their honorable assets by acting opportunistically (Chiles and McMackin, 1996).

It is suggested that there might be some type of infrastructure-based trust factor at play, such as '*Trust in the Internet'* (Jarvenpaa et al., 2000, p. 61). Such a factor would be somewhat related to Luhmann's notion of system trust[43], or Zucker's concept of background institutional trust[44] , which would

[42] For more about institutions see the New Institutional Economy by Oliver Williamson and Ronald H. Coase Williamson O. E. (1975). Markets and Hierarchies: Analysis and Antitrust Implications. NY: Free Press.; Williamson O.E. (1985). The Economic Institutions of Capitalism. Firms, Markets, Relational Contracting. Free Press, New York; Williamson O.E. (1993). Opportunism and its Critics. Managerial and Decision Economics 14 (2), 97-107; Williamson O.E. (2000). The New Institutional Economics: Taking Stocks, Looking Ahead. Journal of Economic Literature 38(3), 595-613; and Coase R.H. (1937). The Nature of the Firms. Economica 4, 386-405.

[43] See N. Luhmann (1979). Trust and Power. John Wiley and Sons.

be affiliated with the participants' overall propensity to trust businesses on the Internet or a certain group of services on the Internet. Researchers have spelled out the factors that potentially affect the user's decision to visit a certain health Web site. For example, The Utilization Review Accreditation Commission (URAC) released the results of a survey of consumers' attitudes towards health Web sites and accreditation (URAC, 2001a). The results strongly suggest that consumers have significant concerns with many health Web sites and that accreditation will help to address those concerns. Only 16 percent of consumers report a high level of trust in health insurance Web sites, and one in four reports a low level of trust. Hospital Web sites fare somewhat better – one-third of consumers report high trust levels and 5percent low levels. According to the survey, 76 percent of the respondents say a quality "*seal of approval*" was extremely or very important for health Web sites. Only one in five respondents say they prefer that the federal government take responsibility for assessing the quality of health Web sites. Three in four say they place the most trust in an independent non-profit organization, and only 5 percent said they trust the Web site sponsors to perform this oversight function themselves. In a more general survey conducted for Consumer WebWatch, 80 percent of Internet users said it is "*very important*" that a site be easy to navigate. Just one in five Internet users said that a seal of approval is "*very important*" when it comes too deciding whether to visit a site (Princeton, 2002).

3.1.3 Expectation of Privacy

> *"I would argue that from the start, the world-wide-web was a transparent rather than a sheltered environment ... given the lack of any clear social norms or laws that control access to Internet wanderings, it is therefore unreasonable to expect privacy in this domain."*
> *(McArthur, 2001, p. 126).*

The HIPAA analysis of Choy, Hudson, Pritts and Goldman (2001) shows that many who engage in online health activities will fall outside the scope of the

---

[44] See L.G. Zucker (1986). "Production of Trust: Institutional Sources of Economic Structure, 1840-1920", in: Research in Organizational Behavior, 8, eds. B.M. Staw and L.L. Cummings (JAI Press, 1986): pp. 53-111.

regulation. It is believed that the application of the regulation on the Internet will be very uneven. Individuals may assume that their health information is protected when it is not. Continued diligence will be required of those online consumers who value their privacy. For example, one of the more controversial aspects of the privacy rule is that it permits the use of health information for marketing purposes without the patient's affirmative, informed permission (Choy, Hudson, Pritts and Goldman, 2001, p. 11). An online health provider that is not covered by the regulation can compile and sell patient lists, subject only to the restrictions of its own privacy policy.

But if there are problems with the practices of online companies, do consumers use sensible strategies to separate the good from the bad? The Medical Library Association recommends that searchers identify each site's sponsor, check the date of the information posted, and verify that the material is factual information, not opinion. The California HealthCare Foundation recommends that consumers take ample time to search for health advice and visit four to six sites. Advocates for privacy, such as the Center for Democracy and Technology, recommend reading a site's privacy policy very carefully – and writing a protest email to any site that doesn't post a policy. And although consumers are generally wary about revealing their identity online or having their activities tracked, only about one in five have checked a site's privacy policy (Fox and Rainie, 2002).

In reality, most consumers go online without a definite research plan. Most customers just plunged right in to see what they could found rather than asking anyone for advice about which Web sites to use. The vast majority visits multiple sites when looking for health information and do not have one favorite site. The typical range of sites visited is two to five. The vast majority of customers who visit multiple sites say that, in general, they start at a site like Yahoo or the AOL home page. The minority of customers who visit multiple sites say they are most likely to start at a specialized health site like WebMD.com. The last time they searched for health advice, those who used a search query engine were more focused on getting the information fast than finding a trusted name – about half started at the top of the search results and worked their way down (Fox and Rainie, 2002).

Only about one quarter of consumers follow the recommended protocol on thoroughly checking the source and timeliness of information and are vigilant about verifying a site's information every time they search for health information. These vigilant customers are more likely than other types of customers to say the Internet has improved the way they take care of their health. Vigilant customers are more likely to take their time and visit many

sites during a typical search. Another quarter of consumers check a site's information "*most of the time*". This group seems to approach the search for health information methodically, trusting search engines to some degree, but clicking on a recognized name more often than the other groups (Fox and Rainie, 2002, p. 4). In traditional practices of exchanging information in computer databases, especially in computer-merging techniques, the primary kind of information exchanged about customers has been confidential information, such as the individual's financial or medical records (Tavani, 1999a). The medical records should be treated confidentially, and medical information is increasingly protected and expectations for its privacy are therefore increasing reasonably (McArthur, 2001, p. 127). Furthermore, "*consumers generally start their searches in a confident frame of mind – and this might be the reason that so many avoid digging into the background of information they are retrieving*" (Fox and Rainie, 2002, p. 17). About one in three customers has bookmarked health-related Web sites or saved them as "*favorite place*" for consultation again and again. Frequent and enthusiastic customers are more likely to have health-related bookmarks, as are those who saw a doctor in the past year. When asked if they have one favorite site, 14 percent of customers said yes. Members of that small group named sites that included, for example, WebMD, the National Institutes of Health and DrKoop.com (Fox and Rainie, 2002).

A key detail of the Internet is that there is no such thing as "*absolute privacy*". Is it therefore reasonable to expect one's Internet browsing to be private or is it reasonable to expect one's email to be private? McArthur (2001, p. 126) argues using the negative voluntary principle as well as the mischance principle, that the answer to those kinds of questions is 'no'. "*It is now well-known that through the use of cookies and other software, the progression of Web sites that one visits in any internet session can easily be tracked.*" All well-documented exposures of email messages suggest that there is little dependable privacy in this realm. "*Therefore, once again by the negative voluntary principle, using email in the face of this legendary insecurity exposes whatever one may write to the eyes of others – perhaps many others. It is not reasonable to expect privacy in email, given all of this permeability*" (McArthur, 2001, p. 127).

Rachels (1975) dissociates the abuse of personal information from the issues of privacy. Rachels is not the only philosopher to approach the abuse of information in this way. Sissela Bok (1983) discusses issues such as the abuse of medical records, and the potential for embarrassment or blackmail when sensitive information is disclosed. Bok analyzed the need that businesses and

governments have to shield certain activities from the scrutiny of the public, and weighed this need against the public's right to know. The title of Bok's book was not 'Privacy', but 'Secrets'. Though some of the topics in the book do bear on Warren and Brandeis-style rights to privacy, Thompson (2001, p. 14) thinks that Bok basically had it right. What is ethically problematic and interesting in all these cases is more precisely captured when we ask whether secrecy can be defended against a general presumption toward publicity. In many of Bok's (1983) and Rachel's (1975) examples, secrecy is defensible exactly when we can show that basic rights of personal security and protection of property would be jeopardized without it.

Consumers are increasingly worried about the loss of their privacy, and have heightened concerns when it comes to their health information. Individuals have a great deal of personal information and sensitive health information in the course of obtaining health care, yet there is little legal protection for health information – online or offline. They worry that their health information may be used or disclosed inappropriately and leave them vulnerable to unwanted exposure, stigma, discrimination, and serious economic losses. They fear that their personal information will be used to deny them health insurance, employment, credit, and housing. As a result, consumers sometimes take drastic steps to keep their health information private. According to a 1999 survey, almost one in six American adults has taken extraordinary steps to maintain the privacy of their medical information. They withhold information from their doctors, provide inaccurate or incomplete information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by their insurance, and even avoid care altogether (Princeton, 1999).

There may be innumerable reasons why customers want to keep their information private, but there are many cases where agents bent on harm can be stopped or slowed in their progress when vital information is not readily available. Many cases illustrate why people may wish to keep fairly unexceptional bits of information as well as sensitive health information out of the hands of those who will use this information in a harmful manner. Information technology has multiplied the types of information that might be so abused, and they have created many opportunities for clever people to obtain such information and to exploit it with little chance of detection. Although this is a fairly unexceptional observation, it undoubtedly covers a significant proportion of the cases where information technology is alleged to threaten personal privacy. In many cases, it is secrecy in the interest of personal security that is at issue, and nothing more. Information technology

has an enormous effect on the ease and speed with which malicious intent can be realized (Thompson, 2001).

Additionally, there is one other consideration that should be noted when considering the probability that harm will occur. Harm might be counterbalanced by the possibility that the affected party will receive benefits (Thompson, 2001, p. 16). Maybe the ethical significance of beneficial outcomes should be included in discussions of trust and opportunism, and therefore we will later discuss the use of the data mining results of genetic information in the spirit of the justification of exception principle. We should not, however, presume that beneficial outcomes can always be used to counterbalance harmful outcomes in any straightforward manner.

The growth of the business-to-consumer and government-to-consumer sectors, where stakeholders are many and unknown, involves emphasis on ways of reducing uncertainty in the online practices. As a general matter, how much privacy customers have and can reasonably expect to have is a function of the practices and laws of society and underlying normative principles. The rapid advance of the Internet has mounted serious challenges to customers' intuitive sense of privacy (McArthur, 2001). Steps to protect privacy must take note of the technological developments and many other issues as well. Sorting through all of this is obviously a complicated matter, but the presented balanced privacy framework is a useful guide to reasonableness as customers struggle to ascertain how much privacy to expect.

3.1.4 Visible and Invisible Privacy Management Practices

This section discusses visible and invisible privacy management practices. From the perspective of the balanced privacy framework, visibility is an important factor for informed consent and rational decision-making.

Visible privacy practices are performed in such a way that an average Internet user is aware of data collection while accessing Web sites with a browser using default security and privacy settings. In visible privacy management, the rules and conditions governing private situations should be clear and known to the persons affected by them, and if a customer chooses to decrease the relative amount of privacy for herself/himself in that situation, she/he decreases the reasonableness of any expectation that this privacy will be observed.

Invisible privacy practices are performed in a hidden manner that requires users to take a proactive role in learning about Web site privacy practices (e.g.

reading the privacy policy, setting the browser's security and privacy settings, learning about cookies, etc.). Although customers are generally wary about revealing their identity online or having their activities tracked, only about one in five have checked a site's privacy policy. This is one of the reasons why some of the privacy policy statements are classified as invisible privacy practices. Customers, however, want their privacy protected and they do not want to be misled by hidden tactics that can undermine privacy.

The concern about privacy is justified, because whenever an Internet customer visits a Web site, a large amount of customer information may easily become available to the Web site owner. The majority of data exchange between a customer and an Internet service is visible to the customer, but there are many methods in which the Web site can gather information without the customer being aware, including cookies and data-mining.

The author has summarized the properties of these two visibility categories in Table 2. Visible and invisible privacy practices are essential trust factors for organizations that participate in online business due to the capability to easily collect data in both visible and invisible ways. Subsequently, consumers provide personal information in either a conscious or unconscious manner.

Table 2: Properties of Visible vs. Invisible Privacy Management Practices.

Visible	***Invisible***
Information voluntarily given, shared, and used	Information collected, used, and shared without consent
Conscious process, easy to conclude	Unconscious process, difficult for consumers to conclude
Open, choice, consent	Closed, hidden, without consumer's knowing consent
Forms, Emails, Surveys	Cookies, Log-files, Server Files, Data Mining

Internet companies learn plenty about Internet customers using invisible privacy management practices. For example, online health providers are able to gather information by depositing cookies. Cookies are bits of encrypted information deposited on a computer's hard drive after the computer has accessed a particular Web site. The Web site stores these bits of information so that when the same site is accessed again by that same computer, the Web site can recognize the computer and provide the same layout, shopping cart, search information, or even the user's name with the exact personalization each time the site is visited. (No reliable figures exist about how many Web

sites install cookies). Some cookies track the activities of a customer at a particular Web site. Others can track the user from Web site to Web site (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 7). Netscape created cookies in 1994 as a special browser feature to make life easier for people browsing the Web. But cookies also allowed the site owner to observe which displays attracted the consumer's attention and which needed some sprucing up. After the media reported on the technology in January 1996, Netscape added a tool to disable cookies for the next version of their Web browsing software. But it was not very easy to accomplish the disabling. Web site users had cookies implanted on their machines unless they took affirmative steps to reject cookies – a classic "*opt-out*" scheme. Most people do accept cookies because standard advice in the privacy section of Internet Web sites is "*Set your web browser to accept all cookies*". It is also the default setting of most browsers, and it is reasonable to assume that most Internet users do not change the setting. Since most people do accept cookies, online companies can easily keep a record of Internet wanderings (McArthur, 2001, p. 126).

The core value framework of privacy entails that if an online company collects a lot of personally identifiable information without consent (which doesn't harm its customer when it collects, stores, and manipulates), it seems to be doing something intrinsically wrong. Moreover, a 2002 survey[45] in the U.S. revealed that 98 percent of Internet users want a Web site to disclose how their personally identifiable information will be used.

Almost 90 percent of Internet users are in favor of "*opt-in*" privacy policies that require Internet companies to ask people for permission to use their personal information. Therefore Internet companies should ask people for permission to use their personal information using visible privacy management practices, which is the kind of system has been adopted by the EU. However, this view challenges the policy negotiated by the Federal Trade Commission and a consortium of Web advertisers, which gives U.S.-based Web sites the right to track Internet users unless the users take steps to "*opt out*" of being monitored. An "*opt-out*" scheme would compel consumers to take steps to protect their privacy (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 3).

Interactivity is a pivotal and much debated concept used to evaluate the overall quality and responsiveness of the Internet. Zemke and Connellan (2001) suggest that electronic commerce will rise or fall on the quality of service that is offered to customers. Therefore it is important to use

[45] http://www.theprivacyplace.org

interactivity possibilities efficiently. Internet companies can increase visibility privacy management using the interactivity properties of the Internet.

Definitions and operationalizations of interactivity vary depending on the context and the medium. Rogers (1995) understood interactivity as the degree to which participants in a communication process can exchange roles and have control over their mutual discourse. Laurel (1991) likened interactivity to the common interface enjoyed by theater audiences and actors, where both parties influence and shape the communication outcome. Likewise, Rafaeli (1988) distinguished between variable degrees of medium responsiveness, recognizing two-way (non-interactive) communication, reactive communication, and fully interactive communication. Building on previous definitions, Ha and James (1998) conceptualized interactivity on commercial sites on the basis of five dimensions: playfulness, (availability of) choice, connectedness to the audience, ability for information collection, and reciprocity.

Media richness theory (Daft and Lengel, 1986) points out that different media can be placed on a continuum of rich and lean communication on the basis of four properties: the ability to transmit multiple cues, immediacy of feedback, use of natural language, and personal focus of the medium. Based on the media richness theory, El Sawy, Eriksson, Raven and Carlsson (1999) suggest that richer media should be used to a larger extent for collaborating, and that less rich media should be used to a larger extent for informing. Additionally, the media richness theory suggests that a rich media is suitable in situations and activities with high uncertainty, while a lean media can be used in situations and activities with low uncertainty. In order to efficiently complete an ambiguous (equivocal) activity, an information-rich medium is suitable, because the activity requires clarification and verbal discussion. As uncertainty is defined as a lack of information, the uncertainty of an activity consequently decreases when more information is received.

Building on the previous definitions, the author has conceptualized interactivity on health Web sites on the basis of previous interactivity definitions, media richness theory and the balanced privacy framework. In this study, interactivity has been understood as the degree to which the customer has the opportunity to choose and *"manipulate" in terms of the* Web site and online health service and privacy process. High interactivity means richer media, a more conscious and open data process, more choices, and more predictable consequences. Interactivity combines the elements of connectedness to the audience, use of natural language, ability for information sharing and informed consent, and reciprocity. Web site interactive content

can add considerable value for both the company and its customer, an issue that is discussed in the following sections.

3.1.5 Data Mining

Next, we explore one important invisible privacy management practice in more detail, because it has been argued that certain data mining techniques, whether used in data warehouses or on the Internet, to extract information about individuals raise serious concerns for privacy. This is because data mining technology can combine information from many diverse sources to create a detailed "*data image*" about each of us, our family, our health interests, our buying habits for medicine, and other interests.

Pearson (2003) points out that "*data mining and data matching can give governments and businesses powerful, useful, and sometimes disturbing new capabilities*." And many analysts believe that the Internet is a 'gold mine' for extracting personal data (Etzioni, 1996; Fulda, 1998), although some analysts see that the Internet plays a minor role in data mining (Inmon, 1996). Tavani (1999a) argues that data mining techniques, which go beyond those concerns introduced by traditional informational-retrieval techniques such as computer merging and computer matching, are incompatible with current data protection guidelines and privacy laws. Although privacy concerns raised by data mining may share many similarities with privacy concerns raised by traditional database retrieval techniques, he points out that there are new arguments to consider. In data mining, the information about persons extracted from a database is not necessarily explicit in the records contained in the database. Instead, implicit patterns and associations are discovered among the data that reside in the database. The data-mining process entails the use of 'open-ended' queries to discover information on relationships and associations about customers. For example, it is possible to simply conduct a query with a request or command such as "*show all patterns*" or "*show a category of trends/relationships*." Companies who practice data mining cannot always predict what uses the resulting information will have. Since data mining is based on the extractions of unknown patterns information from a database, organizations cannot know at the outset what kind of potentially valuable

personal information or what kinds of relationships will emerge from (Tavani, 1999a)[46].

Online companies that interact using the Internet have many possibilities to collect sensitive information using invisible privacy management practices, and thereafter use customer information guilefully. For example, cookies themselves are not inherently bad or necessarily invasive to one's privacy. They are instrumental in activating some of Web's most appealing features. By following customer's surfing around a Web site, the online company is making inferences about what that person might be thinking and looking for. Interference with privacy for the purpose of gathering more information about one's thoughts in order to intervene with the autonomy of decision-making is the kind of interference that many would identify as being the most disagreeable in terms of privacy invasion (Michelfelder, 2001). But it is Web sites' ability to glean user's tastes and lifestyle through cookies that has led to the current debate about the appropriate ways to do tracking and maintain the privacy Americans want. In the most comprehensive and extreme cases, a Web company could build a sensitive profile of an Internet user (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 8).

One "*hidden*" problem that new technology of the Internet poses is expressed by Fulda (1997, p. 28) when he asks: "*Is it possible for data that does not itself deserve legal protection to contain implicit knowledge that does deserve legal protection and, if so, what balance must be struck between freedom to use whatever knowledge one has at one's disposal to further one's own ends and the freedom not to have one's personal data mined into knowledge that will be used as a means to someone else's ends*."

Cavoukian (1998) believes that one interest of data mining is to explore the unmapped terrain of the Internet. She points out that the Internet is becoming an "*emerging frontier for data mining*". Access to an Internet server makes it possible to transfer the data into a data mining process from the Internet server. Data mining is both a powerful and profitable tool for large data pools. For example, by carefully examining Internet transactions of customer purchases and activities, online companies can identify profitable customers and win more of their business. Likewise, companies can use this data to

[46] See more Edelstein H. (1996). Technology How To: Mining Data Warehouses. Information Week (January 8).; Cavoukian A. (1998). Data Mining: Staking a Claim on Your Privacy. Information and Privacy Commisioner's Report, Ontario, Canada.; Bigus J. P. (1996) Data Mining With Neural Networks. McGraw-Hill, New York.; Fayyad U., G. Piatetsky-Shapiro and P. Smyth (1996). The KDD Process for Extracting Useful Knowledge from Volumes of Data. Communications of the ACM, 39 (11): 27-34.

identify non-profitable customers (Clemons and Weber, 1994). Before data-mining techniques were employed in large databases, customers might have had a false sense of comfort regarding personal information about themselves, believing that there might be too much data to be analyzed intelligently. Data mining technology makes it possible for terabytes of data containing personal information to be examined for meaningful patterns (Tavani, 1999a). Information is recorded and stored in databases and subsequently manipulated in ways that produce information patterns and profiles that would not have been possible to acquire in earlier informational-retrieval techniques in databases.

Data can be more conveniently analyzed across the enterprise by using a data warehouse. A data warehouse is a database with tools that stores current and historical data of potential interest throughout the company. The data originates in many core operational systems and external sources. A data warehouse system includes a range of ad hoc and standardized query tools, analytical tools, and graphical reporting facilities. These systems can perform high-level analysis of patterns or trends, but they can also drill into more detail where needed. Companies can build enterprise-wide data warehouses where the central data warehouse serves the entire organization, or they can create smaller, decentralized warehouses called data marts. A data mart is a subset of a data warehouse where summarized or highly focused portion of the organization's data is placed in a separate database for a specific population of users. For example, a company might develop marketing and sales data marts to deal with customer information. A data mart typically focuses on a single subject area or line of business, so it is more secure and restricted than an enterprise-wide data warehouse. Although a data mart is more privacy protective, the problem is that complexity, costs, and management problems will arise if an organization creates too many data marts (Francett, 1997).

Data warehouses not only offer improved information, but also an increase in vulnerability, because they make it possible for many persons and business partners to obtain information widely. They even include the local ability to model and remodel the data. Cavoukian (1998) notes that although data warehouses are not essential to the data mining process, the mining potential of data can be significantly enhanced when the appropriate data is stored in a data warehouse. Data warehousing makes it possible to manage data from a single database. Data warehousing introduces greater efficiency to the data mining process, which has also resulted in that process becoming more economical for organizations that elect to adopt it (Tavani, 1999a). Data

warehouses are typically used for processing transactional information for sales and marketing.

The Internet may be a potential advantage but also a potential threat to privacy for data mining in the context of electronic commerce. Data mining causes privacy concerns because Internet users are often not aware of data mining practices in advance. Data for which they may have given their consent for collection and use in one context is being mined, in ways they had not explicitly authorized, into information and knowledge that is useful to certain businesses and organizations. Even though customers might have explicitly authorized information about themselves to be collected for use by online companies in one context, it does not follow that the customers have also given consent for such information to be subsequently mined for further use and analysis (Tavani, 1999b). This means that the company has converted visible privacy management practices are converted into invisible privacy management. Nissenbaum (1997) uses the term *contextual integrity* to describe the situation where organizations use the information in a context that is not the same as that for which the data was originally gathered.

The preceding points focused on the transactional data, but there is also another good information pool for data mining. Personal information mined from the Internet need not be transactional. Most of the information on the Internet about an individual who is not a public figure is there 'by his leave'. What makes this so important and in what way does it differ from the goal mining process of data warehouses or transactional data? In so far as data warehouses are used as the source from which personal data is mined, privacy concerns surrounding data mining would clearly seem to be an instance of information privacy. One critical distinction between personal information extracted from a data warehouse vs. that which is extracted from the Internet home pages, however, is that in data warehouses the personal information extracted is protected from public view, whereas personal information extracted from home pages is originally available for public viewing. Many guidelines of informational privacy have linked protection to increased control over personal information. But new threats to informational privacy online suggest a need to understand more deeply how informational privacy is not solely a matter of having control over personal information (Tavani, 1999a).

In the stream of enduring public fascination with the Internet, personal home pages represent one of the latest trends. Growing numbers of people develop and maintain personal web pages to present aspects of their personalities online (Papacharissi, 2002). There are millions of home pages containing all the information the home page owner has chosen to reveal and

publish (Fulda, 1998). A national survey by the Pew Internet & American Life Project found that more than 53 million American adults have used the Internet to publish their thoughts, respond to others, post pictures, share files and otherwise contribute to the explosion of content available online (Lenhart, Horrigan, Fallows, 2004). Personal home pages present a new channel for mass communication. As Dominick (1999, p. 647) points out, "*prior to web pages, only the privileged – celebrities, politicians, media magnates, advertisers – had access to the mass audience*". Hosting a personal home page allows people to present a more multi-mediated self, using audiovisual components together with text to communicate to potential mass audiences (Papacharissi, 2002).

A Web page provides the ideal setting for allowing maximum control over the information disclosed. Furthermore, "*most personal Web pages did not contain much personal information, and strategies used for self-representation online were similar to those used face-to-face*" (Papacharissi, 2002, p. 645). It would seem that this kind of information does not need special protection, because much of it seems initially to be harmless or non-controversial. Much of the information related to what an individual does in public can be considered public and unrestricted rather than private and restricted information. Dominick's (1999) content analysis of personal home pages found that the typical page had a brief biography, a counter or guest book, and links to other pages. He viewed these links on personal home pages as a means of social association. But "*by providing links to other sites – i.e. by listing their interests – people indirectly defined themselves*" (Papacharissi, 2002, p. 645).

Fulda (1997) points out that the "*anything put by a person in the public domain could be viewed as public information*" – rule applied well before data was mined to produce new profiles and patterns. Data mining programs can "*learn*" to interpret the content associated with common HTML tags[47] (Fulda, 1998). Some other analysts have also clearly pointed out that there are other techniques, for example intelligent agents and learning techniques (Eisenberg, 1996; Etzioni, 1996), which are able to uncover general patterns regarding individual Web sites and their users. "*Data mining techniques that currently raise privacy concerns about data warehouses may very likely soon raise such concern on the Internet ... thus far; much of that information included on the*

[47] HTML, Hypertext Markup Language, is a page description language for creating hypertext or hypermedia documents such as Web pages. HTML uses instructions called tags to specify how text, graphics, video, and sound are placed on a document and to create dynamic links to other documents and objects stored in the same or remote computers. (See more Laudon and Laudon 1999 p.192, 271).

Web has not yet proved to be a practical repository for those that mine personal data ... however that may soon change." (Tavani, 1999a, p. 140). Tavani states that many of the privacy concerns regarding data mining on the Internet do not seem to be so much involved with personal information related to confidential or intimate matters (for example, information that includes one's medical records or bank records) "*rather, issues arise because seemingly harmless pieces of information about persons can be excavated from an individual's online activities and used in a way to construct a profile of an individual based on information freely put by that individual on the Web for use in a particular context*" (Tavani, 1999a, p. 140). This progress will probably lead to individuals becoming more cautious and even giving some incorrect information on their home pages as more and more personal information is successfully mined from Web sites. Even now they should be more selective about which pieces of personal information they are willing to include in personal home pages as well as on the pages in related Web sites that they may also happen to maintain (Tavani, 1999a). It is important to realize that when this public and unrestricted data is merged with transactional and personal information to produce new profiles and patterns, privacy concerns are widely justified.

3.1.6 Summary

So far we have discussed how enriched health information is processed and what kind of vulnerabilities this might evoke. The Internet has become a major catalyst for both electronic commerce and electronic business, and it is being taken into usage in the health care segment at in increasing pace. The Internet is an effective tool for receive and share data. Since more people are involved in the health process, each person may be involved with sensitive information. Leavitt's Diamond, situated actions, and the unpredictable nature of articulation work were presented because many changes and uncertainty issues reflect on the consideration of the privacy situation. There are many potential privacy threats in sequences of activities.

Sharing personal medical and health information across the Internet requires a certain leap of faith – or at least a strong sense of privacy and trust. In a virtual world, the issue of trust gets magnified, because trust is a critical factor in any relationship in which consumer does not have direct control over the actions of the online company, the decision is important, and the environment is uncertain. The medical records should be treated

confidentially. Medical information is increasingly protected. The expectations of its privacy are therefore increasing reasonable, but a key detail of the Internet is the fact there is no such thing as “absolute privacy”. The rapid advance of the Internet has mounted serious challenges to customers’ intuitive sense of privacy. Customers are increasingly worried about the loss of their privacy. Customers reveal a great deal of personal information and sensitive health information in the course of obtaining health care, yet there is little legal protection for health information – online or offline. They worry that their health information may be used or disclosed inappropriately. As a result, consumers sometimes take drastic steps to keep their health information private.

The concern about privacy is justified because whenever an Internet customer visits a Web site, a large amount of customer information may easily become available to the Web site owner. Internet companies know plenty about Internet customers using invisible privacy management practices. One important invisible privacy management practice, data mining, is explored in more detail because it can give governments and businesses powerful, useful, and sometimes disturbing new capabilities. From the perspective of the balanced privacy framework, visibility is an important factor for informed consent and rational decision-making. Internet companies should ask people for permission to use their personal information using visible privacy management practices. This view challenges, however, the kind of system that has been adopted by the US. An “opt-out” scheme would compel consumers to take steps to protect their privacy.

The Internet has created a new set of management challenges, which will be discussed next.

3.2 Privacy and Service on Demand

3.2.1 Different Scenarios

Many Internet customers are concerned about the privacy issues of electronic commerce and, in contrast, some customers value Web sites that are able to offer a personalized browsing experience due to the information that they collect about customers for their Internet service. The vast majority of American Internet users want the privacy playing field tilted towards them and

away from online companies. They think it is an invasion of their privacy for these businesses to monitor users' Web browsing. By a two-to-one margin they reject the argument made by some companies that Web tracking can be a helpful. However, the majority of customers are willing to share personal information under certain circumstances. Only one in three are hard-core privacy protectionists and would never provide personal information. Advocates of cookie make the case that consumers will eventually come to appreciate cookies because they allow sites to provide information that is important and relevant to an individual Web user. In the case of advertising and marketing, cookie advocates argue that there is a great deal of waste that everyone hates in mass marketing through the mails (junk mail) and the media. These advocates argue that the ideal world created by cookies and tracking is one where the clutter of information and advertisements is cut to a minimum and only useful material is put into users' and consumers' hands (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 2). This section discusses possible scenarios to choose in that situation.

It seems inevitable that Internet companies will know more about customers. The Internet has reduced the normal social buffers that allowed businesses many years to adjust to competition. Rapid changes fueled by the Internet are creating new situations where existing laws and rules of conduct may not be relevant. New "*grey areas*" are emerging in which ethical standards have not yet been codified into law. A new system of ethics for the information age is required to guide individual and organizational choices and actions. Pearson (2003) presents six possible scenarios to choose in that situation. The starting point is *the Today-Scenario*. Typical to the scenario is that there are many disparate and unconnected databases. Additionally, conflicting and uneven privacy protections are industry or government-led. There are fears about identity theft and terrorism because no widespread authentication scheme is provided. This scenario is prevailing, because there is a lack of investment in security and privacy issues; a lack of industry cooperation on privacy infrastructure; and no evolution of current privacy and security policy approaches. Considering the Today-Scenario, it seems that we should change our practices and policies but which way?

According to Pearson, the first alternative is *the 1984-Scenario*, where organizations (government and business) know all about citizens and customers. In this scenario, individuals have no control over the data and information organizations collect. This scenario might happen because of anti-terrorism initiatives and fear of crime and instability. If government rules force e-businesses to divulge personal data and business aim (and they are

allowed) for efficiency only, then this seems to be the only road to follow. From the perspective of this study, this scenario seems to be out of the question. It goes against the core value framework of privacy and the balanced privacy framework. So it seems to be out of the question.

The second alternative is *the Transparent Society-Scenario*, where everyone knows everything about everyone and individuals have given up on privacy. It is like a "*global small town*" and everyone can "*watch the watchers"*. Pearson states that this scenario might happen because of fear of crime and terrorism or the desire for a closer community. From the perspective of this study, this scenario demands fundamental change in attitudes about privacy (starting with exhibitionist teenagers). Although the attitude change of privacy is possible it goes against the core value framework of privacy and the balanced privacy framework. Additionally, this scenario is an impractical and unrealistic choice for electronic commerce.

The third presented alternative is *the No Control-Scenario*, where systems are insecure and hackers can break into almost any system. Hackers post and publicize that data they find. This might happen because of buggy code and lack of IT and telecom industry cooperation. Additionally, there is much complexity and sloppy maintenance. From the perspective of this study, this scenario seems to be a very unrealistic choice because there are so many law statutes and directives available. This scenario does not reflect trust at all, and therefore there would be little e-business and e-government.

The fourth alternative is *the Chaum's World-Scenario*, where customers refuse to share personal identity. Anonymous transactions are the norm in this scenario. This might happen because of new anonymizing technologies and bulletproof privacy rights management tools within workable business models and increased concerns about privacy. Many business and industry representatives in the electronic commerce sector suggest that virtually all privacy issues, including those generated by data mining, can be resolved through certain technical solutions (Tavani, 1999b). "*The ability to hide your true identity gives mistrusters a defense mechanism on the Internet that is not so easily available in the real world*" (Uslaner, 2000, p. 19). The use of online deception tactics such as fake names highlights the compartmentalization that is the basic tool of people who want to control their privacy. But there is no single answer to how privacy-enhancing technology can manage privacy issues widely, because technology will enable online companies and customers to be more responsive, productive, innovative, and resilient. Certain technologies pose new privacy concerns, depending on how they are used (Pearson, 2003). From the perspective of this study, using anonymity in the

health service process is not a convenient practice because it might be even a threat to sufficient health operations. "*To shield themselves from what they consider harmful and intrusive uses of their health information, customers have engaged in privacy-protective behaviors, such as providing incomplete information, thereby putting themselves at risk from undiagnosed, untreated conditions. The lack of complete and accurate health information on patients impacts the community as well. Health care information used for important research and public health initiatives downstream becomes unreliable and incomplete.*" (Choy, Hudson, Pritts and Goldman, 2001, p. 1).

The last presented alternative is *the Trusted Balance-Scenario*, where customers feel comfortable having certain governments and trusted businesses "*know all about the customer*", because individuals know who has his/her data and how it will be used. The data is well protected against unauthorized use and individuals can decide what to share and when. This scenario might happen because of efficiency and customized service from electronic business organizations on demand. Anti-terrorism initiatives are also pursuing this scenario. Additionally, this requires effective privacy rights management tools and industry-wide commitment to real security. According to this scenario, companies are competing to give customers the privacy they want. If we consider the balanced privacy framework, the core value framework of privacy, and the advantages and threats of electronic commerce but also the possibilities in the global setting, the trusted balance scenario seems to be a very suitable path to follow in terms of electronic commerce. It is, therefore, chosen as the starting point to develop a more practically-oriented model. It is further developed in this thesis on the basis of the balanced privacy framework and empirical studies of healthcare privacy policies. This further developed scenario and perspective is called *The Balanced Privacy Model* from this point on.

3.2.2 Balanced Privacy Model

A standard way of framing the debate over interests involving individual privacy and the implementation of a new technology "*is as an issue calling for a balancing of the needs of those who use information about individuals ... against the needs or rights of those individuals whom the information is about."* (Johnson, 1994, p. 88). Theorists working in sociological traditions have tended to interpret the emergence of computerized information technology as something that enables an evolution in social power relations

that favors governmental and commercial organizations against the interests of individual citizens (Johnson, 1994; Gotlieb, 1995).

Calvin Gotlieb (1995) has criticized sociological tradition perspective on two counts. First, it takes a sweeping approach that neglects the important distinction among the different interests affected by computerization. Second, it downplays the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings. The balanced privacy model contains the possibility to use those needed amendments.

In Figure 5 the author presents a model that considers the customer's and company's interests. Employing an interactive dialog by demanding or consenting, customers are able to choose *Service-on-Demand* and *Privacy-on-Demand* functions accordingly. The Service-on-Demand function may vary from "*rich service*" to "*lean service*" and Privacy-on-Demand may vary from "*publicity*" to "*secrecy*". The interactivity features of the Internet has the ability to make privacy issues more exact to consumers, which in turn enables them to choose privacy practices (P_x) and make more informed decisions concerning to whom they entrust their personal identifier information and what kind of service functions (S_y) they prefer and vice versa. The balanced line BL_1 illustrates normative privacy practices, like law statutes. In that case, the Privacy-on-Demand function has no flexibility available in the privacy situation. An ideal case of normative privacy practice in privacy situation is one where everything is black or white, true or false, without any consideration of customers' values or service function. The balanced line BL_2 illustrates the situation where a customer is able to give informed consent and to make rational decision-making. A customer is able to opt-in (or opt-out) of privacy function and service function accordingly. If the company changes the balanced line (BL_1, BL_2) without consent or demand by the customer, it may be leaning toward opportunism or detracting from electronic commerce business.

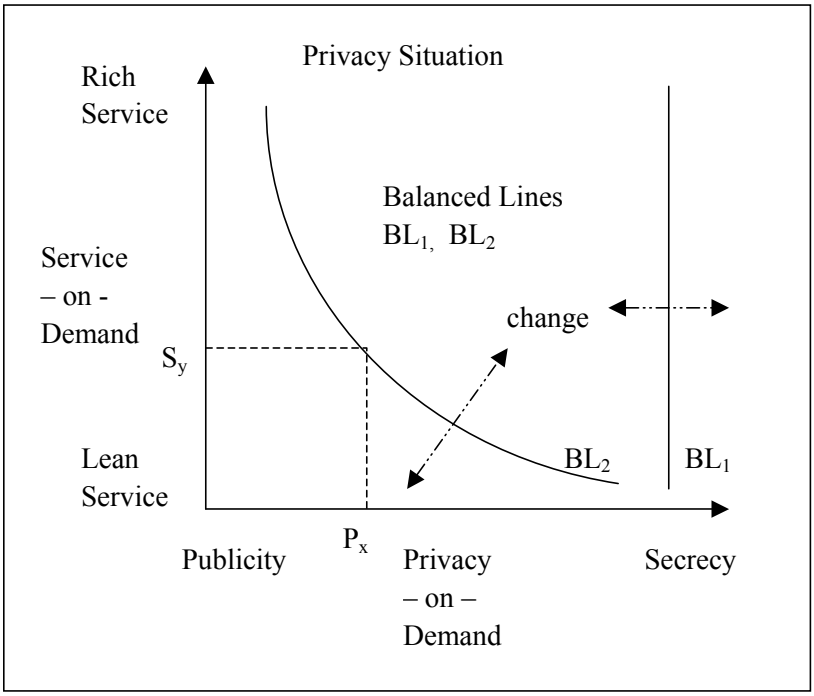

Figure 5: Balanced Privacy Model.

So far we have pointed out that it is neither the kind of data nor the content of the data itself that will determine the privacy matter. Instead, it is the situation in which the knowledge is used that we must consider. Two points are worth considering in the knowledge use situation: one having to do with fairness, and the other having to do with consent. First, because customers are often unaware that personal information about them is being used, we can question whether the data subjects are being treated fairly. Second, because the personal data that the data subjects may have willingly granted for use in one context is often subsequently used for other purposes, there are issues related to authorized consent. Although customers may have consented to the use of certain data about themselves in one context, it does not follow that they consented to that same data being used in other situations, specifically in those situations which they had not explicitly authorized. That is why the term "*Privacy Situation*" is used in Figure 5.

Let us next turn to the question of how to balance the health-related privacy concerns of the various interested parties in the balanced privacy model. The data mining of genetic information is discussed to illustrate the use of the balanced privacy model in a privacy situation.

The ethical questions surrounding genetic information are often addressed in terms of rights. Individuals are supposed to have rights to privacy, confidentiality, nondiscrimination, and autonomous decision-making. It is their right to consent or not to consent to genetic tests, and if their permission cannot be obtained, their best interest should, by right, guide any decisions (Häyry and Takala, 2001).

Suppose a patient decides to get tested for a breast cancer gene. Breast cancer runs in her family, and she wants to know whether she is genetically disposed to have breast cancer. She goes to the laboratory for tests for the gene and the results are positive. The laboratory results are stored in her electronic medical record so that the tests results are available to medical researchers and physicians to encourage aggressive testing for the disease in the future. Because the information will be computerized, it means that many health providers and researchers may have access to the information. For example, if the patient's health insurance company gets access to it, then it could mean problems to the "*owner of the information*". Information of this kind could be detrimental to the customer when obtaining life insurance or future health insurance. Eventually, if the medical information slides through enough networks and information systems, it could be detrimental to the customer's relatives when obtaining insurance and applying for employment even though they have shown no signs of the disease and have never been tested.

Moor (1997, p. 32) supposes that "*new legal policies might be helpful here including the passage of statutes protecting patients from discrimination on the basis of genetic testing."* Choy, Hudson, Pritts and Goldman have pointed out (2001, p. 1) that "*A substantial barrier to improving the quality of care and access to care is the lack of enforceable privacy rules. In the absence of federal health privacy laws, people have suffered job loss, loss of dignity, discrimination, and stigma*." Additionally health providers might consider setting up a zone of privacy for customers who only want predictive testing done because there is, as Moor points out (1997, p. 32), "*a difference between predictive genetic testing in which the patient is tested for genetic information that may be indicative of future disease and diagnostic testing in which the patient is tested for genetic information that may confirm a diagnosis of an existing disease."* The health provider could establish a private situation for predictive testing so that the customer's analyst results were not incorporated into the regular medical file. If we think about privacy issues from the perspective of the balanced privacy model, these medical records would be computerized but not accessible to all of those who have access to the general

medical record. This practice allows adjustment of the access conditions to increase the level of privacy for the patient.

According to the balanced privacy framework, it is clear that customers should be told what will happen to the analysis information. The customers can choose their privacy situation better if they know where the zones of privacy are and under what conditions and to whom information will be given. Rules and conditions governing private situations should be clear and known to the persons affected by them, so customers are able to determine Service-on-Demand and Privacy-on-Demand functions accordingly. The customers might prefer to have the analysis information included in their medical record. So they choose a richer service function but less privacy.

The genetic test gives us also an example that describes the nature of the justification of exceptions principle. Suppose that after some predictive genetic tests are run, new information about the consequences of the analysis results is uncovered by means of the data mining process. The customer's old health information in combination with the analysis results show that the customer surely must have transmitted a devastating disease to her offspring, but that the disease can be treated effectively if caught in time. The physician's duty to keep the patient's secrets confidential is an important protection of privacy and the values related to it, but it is by no means absolute in medical law or ethics generally (Somerville, 1999; Mason, McCall and Smith, 1985).

> *"In the context of genetic information, the most prominent reason for breaches of confidentiality is the harm inflicted on others by their ignorance ... But the strength of arguments like this varies from case to case, depending on the specific nature of family relationships between the individuals involved"*
> *(Häyry and Takala, 2001, p. 408).*

In such circumstances it would seem that the health provider should notify not only the customer but also her adult offspring even though that was not part of the original privacy policy and practice. The breach is justified because the harm caused by the disclosure will be so much less than the harm prevented. Using the justification of exception principle, a health provider may determine the change of balanced line without the threat of opportunism. The interactivity capability of the knowledge sharing of the Internet means many possibilities and opportunities for privacy management practices. The Internet can be used to build closer relationships with customers.

The adjustment principle in this example states that those who continued to have predictive genetic testing would know what information would be

released in stated exceptional circumstances. They would know the possible consequences of their decision to have predictive genetic testing and could plan accordingly. According to the adjustment principle, the balanced privacy model should indicate the new privacy practice.

3.3 Conclusion

So far we have commented on the advantages, and weaknesses the Internet has regarding customer information of business processes and practices. At the center of the focus have been new possibilities to conduct health care business and the potential problems for privacy the Internet poses. The Internet provides a universally available set of technologies for electronic commerce that can be used to create new channels for marketing, sales, and customer support and to eliminate intermediaries in buying and selling transactions. There are many business models for electronic health on the Internet, including marketing, publishing, transactional, and interactive operations.

The activity of storing and retrieving personal information has been enhanced to the extent that all of us now have a legitimate basis for concern about the improper use and release of personal information through networks.

Advances in data mining techniques for large databases are a technological trend that heightens ethical concerns, because they enable companies to find out a lot of detailed personal information about individuals. Companies can use the Internet to assemble and combine the myriad pieces of information stored on customers by information technology more easily than in the past. Concerns with informational privacy generally relate not to the collection of information itself, which many consumers would gladly give for appropriate use in a specific situation, but to the manner in which personal information is used, and then disclosed. When a business collects information without the knowledge or consent of the customer to whom the information relates, or uses that information in ways that are not known to the individual, or discloses the information without the consent of the customer, information privacy is seriously threatened.

In general, the amount of privacy customers have and can reasonably expect to have is a function of the practices and laws of our society and underlying normative principles. The rapid advance of information technology has mounted serious challenges to customers' intuitive sense of privacy. New technologies, new products, and changing public tastes and values (many of

which result in new government regulations) put strains on any organization's culture, politics, and people. Because information systems potentially change important organizational dimensions, including the structure, culture, power relationships, and work activities, it is very important to refocus and review privacy and security policy issues in the organization.

It has pointed out that privacy is best understood in terms of the balanced privacy framework in the electronic commerce context. It provides perspectives and principles to consider when we are pursuing the balanced privacy model. The balanced privacy model entails the needed flexibility for electronic commerce but also demanding rules and principles. If privacy is understood not merely as a value involving the good of customers but as one that also contributes to the broader social and organizational good in the light of the balanced privacy model, then the concern for individual privacy might have a greater chance of receiving the kind of consideration it deserves.

4 EMPIRICAL STUDIES

So far we have discussed the theoretical aspects of the demands for good privacy practices of a Web site. In this section, practical privacy policies are analyzed to find out different communication practices of privacy matters and the typical content of a health care Web site privacy policy.

This empirical part of the study includes categories of privacy items that provide an effective mechanism for analyzing and comparing privacy policies, system requirements, and the functionality of the respective systems. Several analyses that focus on health care organizations have guided the development of the frameworks presented in this section. The study incorporates several categories and properties that impact privacy policy content as well as privacy management practices.

Theoretical sensitivity represents an important creative aspect of the used method. This sensitivity represents an ability to use not only personal and professional experience imaginatively, but also literature. Theoretical sensitivity has been used for developing the presented frameworks and models in the preceding sections. The core value framework of privacy, the balanced privacy framework, and the balanced privacy model enable the analyst to see the research situation and its associated data in new ways, and to explore the data's potential for identifying, developing but also reducing items accordingly. This study led to the development of privacy item categories and enabled the codification of a comprehensive set of coding schemes tailored to the content analysis of privacy policies.

4.1 Method

4.1.1 Study Process

In order to identify the typical content of health care Web site privacy policies and to identify used communication practices of privacy matters in health care Web sites, a technique called content analysis was employed to derive the privacy-related items of various Internet health care Web sites. The protection of personal information, such as that managed by health care Web sites, is not an option but a necessity and content analysis is an effective technique for

examining how Internet Web sites claim they manage online customer data and how they convey these practices to their customers. The used method is the culmination of several phases of privacy policy and legal analyses as presented in Table 1. In addition, it has been successfully applied to the analysis of health care Web sites and financial institutions[48]. Using content analysis, it becomes possible to develop a corpus of reusable privacy and security items for Internet service evaluation. Those items are the basic building blocks of the presented study. Items are a cogent unit used to objectively analyze and compare Internet privacy policies, thus enabling us to provide IT practitioners, policy makers, and consumers with useful guidance. Additionally, these items can be used to reconstruct the implicit requirements met by the privacy policies as well.

The research process is summarized in Figure 1 and each of the steps is described below the figure. The author has used the content analysis procedure almost orthodoxically.

> *"The procedures are not mechanical or automatic, nor do they constitute an algorithm guaranteed to give results. They are rather to be applied flexibly according to circumstances; the order may vary, and alternatives are available at every step." (Diesing, 1971, p. 14).*

The study used the privacy policies found on the health Web sites as the texts to be examined, and the analyzed Web sites are presented in Section 4.1.4. The used study process comprises four main activities, which are discussed in the following sections in more detail: item identification, item reduction, category determination, and generation of the coding scheme. Only the coding scheme of major categories is presented. Other coding schemes are presented in the later sections.

---

[48] See the following papers: Earp J.B., A. I. Antón and O.P. Jarvinen (2002). "A Social, Technical and Legal Framework for Privacy Management and Policies," Proceedings of the Eighth Americas Conference on Information Systems (AMCIS 2002), Dallas, Texas, pp.605-612, 9-11 August, 2002. Järvinen O.P., J.B. Earp, and A. I. Antón (2002). A Visibility Categorization Scheme for Privacy Management Requirements. Second Symposium in Requirements Engineering for Information Security, Raleigh, NC, USA, October, 2002. Järvinen O.P. (2003) Privacy Seal Programs and Privacy Policies in Health Care IT-Services. Proceedings of the Combining views from IS and service research seminar, Turku. TUCS General Publication, No 25, June 2003, pp. 41 - 65. Järvinen O.P. (2003) Revision of Privacy Policy: Five Perspectives and ONION-model. People and Computers: Twenty-one Ways of Looking at Information Systems. (ed. Järvi, T. & Reijonen P.) TUCS General Publication, No 26, June 2003, pp. 167 – 184. Antón A.I., J.B. Earp, D. Bolchini, Q. He, C. Jensen, W. Stufflebeam (2003). The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. NCSU CSC Technical Report #TR-2003-14, 1 August 2003. Antón A.I., J.B. Earp and A. Reese (2002). "Analyzing Web Site Privacy Requirements Using a Privacy Goal Taxonomy." 10th Anniversary IEEE Joint Requirements Engineering Conference (RE'02), Essen, Germany, 9-13 September 2002.

4.1.2 Unit of Analysis

The third step of the content analysis is to decide on the type of issue to be counted in the analysis, the so-called "*unit of analysis*". The unit of analysis was chosen to be consistent with the nature of the research question. The study questions to be addressed included the identification of the typical content of a health care Web site privacy policy and typical communication practices of privacy matters, and thus privacy policy statements, which may vary by a couple of words to a sentence, were chosen as the unit of analysis. It is a detailed type of analysis, but it is also very generative (Strauss and Corbin, 1990, p. 72).

After that decision, it was possible to begin by analyzing the privacy policies on a line-by-line analysis. An implication that followed from the research questions and the choice of the unit of analysis was that the data analyses had to be done by hand using human coders. The basic analytic procedures by which items were identified and developed were: asking questions about the data and making comparisons of similarities and differences between each privacy policy statement and other instances of phenomena. This involved close examination, phrase by phrase, and sometimes even of single words.

The Georgetown Internet Privacy Policy Survey found that Internet privacy disclosures do not always reflect fair information practices (Culnan, 1999). This contributes to the inability to categorize all privacy items as simply protective items. Instead, privacy items were categorized as either protective or vulnerability items.[49]

To identify items, each statement in a privacy policy was analyzed by asking the following questions: "*What goal(s) does this statement or fragment exemplify?*" and/or "*What goal(s) does this statement obstruct or thwart?"* The purpose behind the use of questioning was to open up the data: to think of potential items, categories, and their properties[50].

Consider Privacy Policy Statement #1 taken from the National Institutes of Health (NIH) privacy policy:

---

[49] This "major category" and the identifying questions of the major category were originally used by Antón, Earp, and Reese. See the paper Analyzing Web Site Privacy Requirements Using a Privacy Goal Taxonomy, Annie I. Antón, Julia B. Earp and Angela Reese. 10th Anniversary IEEE Joint Requirements Engineering Conference (RE'02), Essen, Germany, pp. 605-612, 9-13 September 2002.

[50] References to particular health Web sites are made to illustrate the potential application and shortcomings of the health privacy practices. They are not legal judgments of policies and practices of specific sites.

Privacy Policy Statement #1:

> *When inquiries are emailed to us, we store the question and the email address information so that we can respond electronically.*

By asking item identification questions, item I_1: `STORE the question and email address`, was extracted[51]. Items are identified using inquiry-driven and traditional action word location techniques. The extracted items are expressed in structured natural language using action words. The identified items are worded to express a state that is true, or a condition that holds true, when the item is realized. This is an extension of previously supported techniques (Abbot, 1983; Rumbaugh, Blaha, Premerlani, Eddy, and Lorensen, 1991; Booch, 1991).

The used technique also suggested two deduction techniques: the action word approach and item reduction approach. To demonstrate the action word approach, consider Privacy Policy Statement #2 taken from the Centers for Disease Control and Prevention (CDC):

Privacy Policy Statement #2:

> *Unless you provide additional information, CDC collects only the following information as you browse through the CDC web site:*
> *- the domain name and browser you use to access the Internet;*
> *- the date and time of your visit;*
> *- the pages you visited; and*
> *- the address of the web site you visited immediately prior to visiting the CDC site.*

The action word COLLECT appears in Privacy Policy Statement #2. This action word serve as an indicator for several items: I_2: `COLLECT domain name`, I_3: `COLLECT browser type`, I_4: `COLLECT date and time site was accessed`, I_5: *`COLLECT the pages visited`* and I_6: `COLLECT the address of the preceding Web site`.

All action words are possible candidates for item identification and the chosen words are called *keywords*. However, all verbs are not keywords. For

[51] The author has used font “courier new” for the clarification of item presentation.

example, consider Privacy Policy Statement #3, taken from the breast cancer site:

Privacy Policy Statement #3:

> *For enhanced user experience, we may attempt to drop a cookie on your computer in order to store your clicking history.*

In this privacy policy, the term "*drop*" is used. The terms "USE" and "DROP" are in this case synonymous and can be reconciled as one term. The analyst can choose either of the two terms. Because the term "USE" is more suitable in other cases, it is chosen. Table 3 presents a version of the keyword list which contains 36 verbs that have been found and used in this study[52] .

Table 3: Privacy Policy Keywords.

Advise	Disallow	Opt-In	Recognize	Store
Allow	Discipline	Opt-Out	Register	Track
Collect	Disclose	Post	Remove	Update
Comply	Keep	Prepare	Require	Use
Connect	Limit	Prevent	Retrieve	
Communicate	Maintain	Prohibit	Sell	
Customize	Monitor	Protect	Send	
Determine	Notify	Provide	Share	

Thus, items in privacy policies may also identified by looking for useful keywords (verbs).

Once items are identified, they are elaborated upon. Item elaboration entails analyzing each item for the purpose of documenting item properties. Properties are important to recognize and systematically develop because they form the basis for making relationships between major categories, categories, and subcategories. Items were considered synonymous if their intended end states were equivalent, or if they meant the same thing to different stakeholders who simply express the item using different terminology.

[52] A larger version of the list contains 57 keywords commonly found in health care and financial Internet privacy policies. See the paper: Antón A.I., J.B. Earp, D. Bolchini, Q. He, C. Jensen, W. Stufflebeam (2003). The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. NCSU CSC Technical Report #TR-2003-14, 1 August 2003, p.5.

To demonstrate item reduction approach, consider Privacy Policy Statement #4 and Privacy Policy Statement #5 taken from the Centers for Disease Control and Prevention (CDC) and from the WellMed:

Privacy Policy Statement #4:

> *CDC does not disclose, give, sell, or transfer any personal information about CDC web site visitors unless required for law enforcement or otherwise required by law.*

Privacy Policy Statement #5:

> *Despite WellMed's efforts to protect your personal information, in certain limited circumstances we may be legally compelled to release your personal information in response to a court order, search warrant, subpoena or other valid legal action.*

Privacy Policy Statement #4 yields tentative item (keyword and properties) I_{t1}: `DISCLOSE personal information if required for law enforcement` and accordingly Privacy Policy Statement #5 yields tentative item I_{t2}: `DISCLOSE personal information in response to a court order`.

Those privacy policies statements are synonymous and can be reconciled as one item that encompasses the spirit and scope of both. The analyst can choose either of the two tentative item names; however, all essential information must be maintained. In the case of these two tentative items, they were further merged with other tentative items. Finally item I_7: `DISCLOSE collected PII when required by law` was chosen to express them all. Thus, if the same item appears more than once, all but one of the items should be eliminated.

Item reduction is part of the content analysis and it is possible to do using the keywords. In the course of the privacy policy study, hundreds of items were discovered. Those items were reduced, documented, and annotated with auxiliary information, including the responsible properties. The list of formally defined keywords provides a useful, extensible vocabulary for examining privacy policies because they standardize what different policies express with different terms in a manner that can increase visibility and understanding for consumers (and researchers). This is discussed in more detail in Section 4.5.

4.1.3 Major Category (Protective vs. Vulnerability) Scheme

The fourth step of the content analysis is to determine the categories into which the items had to be divided, and the fifth step is to generate the coding scheme. Those steps are discussed in this section and the major categories, protective and vulnerability, are determined.

After some deduction, the items were grouped together under a higher order. Certain items were deemed significant because they were repeatedly present or notably absent when comparing privacy policy statement after privacy policy statement. Questions like, "*What is this?"* and "*What does it represent?"* were asked. It was important to think about privacy policies analytically rather than descriptively, to generate provisional categories and their properties, and to think about generative questions. The categories into which the items are to be placed must be grounded in the data from which they emerge and from the theoretical knowledge that the analyst brings to the task (Berg, 1998; Strauss, 1987). In the study, the initial development of categories followed from the questions to be examined and from the account of privacy that had already been established.

Once particular phenomenon was identified in data, it was possible to begin to group items around them, and through the coding procedures they earned the status of categories. Similar privacy items were labeled and grouped. The process of grouping items that seem to pertain to the same phenomena is called categorizing. "*Categories have conceptual power because they are able to pull together around them other groups of concepts or subcategories*." (Strauss and Corbin, 1990, p. 65).

In the first phase of the privacy policy study (see table 1), privacy policy taxonomy was created by Antón, Earp, and Reese (2002). It aimed at identifying privacy policy goals that reflect or contribute to protective or vulnerability matters. Privacy policies should express the ways in which they protect personal information but, according to the Fair Information Practice Principles, Internet companies should also inform their customers of potential vulnerabilities that may threaten one's privacy. According to the taxonomy, privacy protective goals relate to the desired protection of user privacy rights, whereas privacy vulnerability goals relate to existing threats to consumer privacy. The initial empirical studies were done based upon the use of the Goal-Based requirements Analysis Method – GBRAM (Anton, 1997; Anton and Potts, 1998). In this dissertation, the author used content analysis and calls protective and vulnerability taxonomies major categories because other (sub-) categories used in this study can be subsumed under them as properties

and strategies. In addition, the author has developed the basic protective and vulnerability taxonomy concept further by adding theoretical sensitivity for consideration. The core value framework of privacy, the balanced privacy framework, and the balanced privacy model enable the analyst to see the privacy situation and privacy policies in new ways, and thus, to explore in more detail the data's potential for identifying, developing but also reducing major category items.

Protective items are categorized by analyzing each item and asking the basic question[53], *"Does this item potentially foster the privacy and/or security of one's privacy situation?"* Theoretical sensitivity gives us more theoretically-based evaluation criteria to make decisions, and therefore it is important to also consider, *"Does this item support the core value framework of privacy?"* and/or *"Does this item support the balanced privacy framework?"* and/or *"Does this item support the balanced privacy model?"* The additional questions give us more theoretical arguments for the final answers.

Consider Privacy Policy Statement #6 taken from the Aids.org privacy policy:

Privacy Policy Statement #6:

> *At no time does AIDS.org share, sell, or otherwise release any personal information about you.*

This statement yielded the item I_8: `PREVENT disclosing Personal Information.` This item clearly seeks to protect one's privacy and it supports the basic questions and is thus categorized as a privacy protective item. An item which has some of the following privacy keywords, `ADVISE, OPT-IN, DISCIPLINE, POST, COMPLY, LIMIT, PREPARE, REQUIRE, NOTIFY,` or `PROTECT` is categorized as a privacy protective item in every case. For example, all items which included the keyword OPT-IN supported the additional questions strongly.

In contrast to protective items, vulnerability items are those related to existing threats to user privacy. They represent statements of fact or existing behavior and are often characterized by privacy invasions.

---

[53] The author has modified the GBRAM-type question originally presented by Antón, Earp, and Reese (2002), converting it into a content analysis format. The author has also added the consideration of three privacy frameworks to see the privacy situation in more detail and further explore the data's potential for identifying, developing but also reducing items accordingly.

Vulnerability items are categorized by considering each item and asking the basic question[54] "*Does this item potentially compromise the privacy and/or security of one's privacy situation?"* and the more theoretically developed questions, "*Does this item conflict with the core value framework of privacy?"* and/or *"Does this item conflict with the balanced privacy framework?"* and/or *"Does this item conflict with the balanced privacy model?"* give us more theoretical arguments for the final answers.

Consider Privacy Policy Statements #7 taken from the American Cancer Society (ACS) privacy policy:

Privacy Policy Statement #7:

> *ACS has links to other Web sites that are not under its control, and ACS is not responsible for the contents of any linked Web site, or any link contained in a linked Web site, or any changes or updates to such Web sites. This privacy statement applies only to the ACS Web site.*

These statements yielded the item I_9: *ALLOW links to other sites whose privacy policy is different*. This item is categorized as a privacy vulnerability item, because it potentially comprises the privacy and security of one's privacy situation. It does not support the balanced privacy model either, because there is no possibility to OPT-IN/OPT-OUT of the current privacy practice. Item with some of the following privacy keywords, SELL, RECOGNIZE, SEND, COLLECT, DETERMINE, REGISTER, SHARE, KEEP, CONNECT, TRACK, COMMUNICATE, CUSTOMIZE, or RETRIEVE, are categorized as a privacy vulnerability item in every case.

Items which have some of the following privacy keywords, DISALLOW, PROVIDE, ALLOW, DISCLOSE, REMOVE, OPT-OUT, STORE, MAINTAIN, PREVENT, MONITOR, PROHIBIT, or USE, are categorized as either a protective or vulnerability item depending on the properties of the item. For example, item I_{10}: ALLOW customer to modify/remove their PII, is categorized as a privacy protective item (as opposite to the use of the keyword ALLOW, compare I_9). If the customer is able to modify their information, the practice supports the balanced privacy model as discussed in Section 4.2.

[54] The author has changed the original vulnerability concept accordingly.

It is important to recognize and systematically develop properties, because they form the basis for making decisions, for example, the keyword MONITOR is related to both vulnerability and protective items. This is because the incentive to monitor Internet users' behavior is not simply confined to those who want to sell them products and services. There are legal encouragements of social interest to monitor online actions. Business executives can be sued if they do not maintain a safe and harassment-free work environment. That gives these executives encouragement to watch what happens on their computer system (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 14). A safe technological infrastructure of e-commerce is an important matter for customers (and also for companies), and therefore this relative item is categorized as protective in those cases.

There are obvious and visible privacy invasions but also insidious and invisible privacy threats. Some invasions are covert in that they are not readily apparent to the users, as is often the case when non-transient cookies are placed on the customer's data media. This is especially evident when the cookie ads provide no additional value or benefit to the user. There are several kinds of insidious and invisible privacy invasions.

Some may argue that if a consumer opts in to the possibility to use a cookie, the following practices cannot possibly be insidious: having to be monitored, having one's usage patterns data mined, or having one's health-related information stored in a database and/or shared with third parties. However, they do not support the balanced privacy model, because collection of such personally identifiable information presents the potential for insidious and "invisible invasions of privacy" simply because of the vulnerability presented by its existence and, consequently, the potential for abuses. Obvious and visible privacy invasions are those that consumers are acutely aware of or about which they eventually become aware, and therefore they support the balanced privacy model in OPT-IN cases.

There are, however, some interpretative problems of categorizing, because items are not clearly separated in Web site privacy policies. The item reduction and coding scheme coupled with the categories provides a basis for identifying conflicting statements within a privacy policy, but some privacy invasions are benign or at least can be interpreted that way by some customers. The problem is what one customer considers a privacy invasion (vulnerability items) may be a valued feature or service to another consumer. From the customers' perspective, it is important to help customers evaluate and make decisions between practices that protect their privacy and practices that may introduce potential vulnerabilities, and in those cases the balanced privacy

framework and the balanced privacy model gives more exact criteria to evaluate each item accordingly. Attempts have been made to manage interpretive problems by carefully considering each item's actual intent in the spirit of the balanced privacy framework and the balanced privacy model.

4.1.4 Analyzed Web Sites

The sixth step is to conduct a sample or pilot study and revise the categories and coding scheme as needed, and the seventh step is to collect the data. The presented study included several phases and iterations that are discussed in Section 1.5 and presented in Table 1. This section focuses mainly on the seventh step.

The health care segment seems to make a difference in a phenomenon of interest at various Web sites of different health care segments. It resulted from the initial experience of analyzing 23 Internet privacy policies for health care services in three health care segments: pharmaceuticals, health insurance, and online drugstores during Phase 1 and Phase 2.

In order to more precisely to determine those segment differences, privacy policies were collected from five different health care segments for this study. The selection process yielded a total sample of 39 US-based health care companies; a portion of the European Union Directive; and a European Recommendation addressing Internet privacy.

The analysis began with an item-based analysis of the two legislative documents; then each Web site privacy policy was examined and all privacy-related items were extracted and documented. The initial study was coupled with the analysis of 16 health care Web site privacy policies for services in two health care segments: medical institutes and general health information Web sites. All Web site privacy practices were reviewed and the "*final*" results of content analyses are presented in this dissertation.

During the study, the author wanted to absorb and uncover potentially relevant data, items, and categories. Straus and Corbin (1990, p. 62) point out that once the attention is fixed, it is possible to begin to examine and ask questions about those items and categories. Such questions not only describe what we see, but in the form of propositions suggest how the phenomena might possibly be related to one another. Propositions permit deductions, which in turn guide data collection that leads to further induction and provisional testing of propositions. Therefore, it was best not to structure the documents too tightly. Rather, the author wanted to allow sufficient space for

other potentially relevant concepts to emerge, while at the same time thinking about conceptual areas that the author had brought to the investigation or uncovered during the research process. The EU directive and recommendation were chosen because "*technical literature can direct theoretical sampling. The literature can give you ideas about where you might go to uncover phenomena ,..., it can direct you to situations that you may not otherwise have thought of, but that are similar or different from those being studied; thereby enabling you to add variation to the study.*" (Strauss and Corbin, 1990, p. 52). "*By choosing the right literature in tandem with doing analysis one can learn much the broader and narrower conditions that influence a phenomenon*." (Strauss and Corbin, 1990, p. 55).

However, only privacy policies were selected for the final and presented analyses. Items were extracted from the following health care privacy policies: 6 pharmaceuticals companies, 7 health insurance companies, 10 online drugstores, 6 medical institutes/disease specific Web sites, and 10 general health information Web sites[55]. The analyzed Web sites are presented in Table 4[56].

[55] The health care privacy policies were re-examined and were in force during February 2003.

[56] Note that a government agency has .gov in the address, an educational institution is indicated by .edu in the address, a professional organization such as a scientific or research society will be identified by .org. and commercial sites identified by .com will most often identify the sponsor as a company.

Table 4: Analyzed Web sites and Major Category Item Hits.

Sites	Protection Items	Vulnerable Items	Pharmaceutical	Health Insurance	Online Drugstore	Medical Institutes	General Health	Web site
Bayer	9	9	x					http://www.bayercare.com
Glaxo Wellcome	6	7	x					http://www.imgw.com
Lilly (Eli)	2	5	x					http://www.lilly.com
Novartis (Ciba)	20	5	x					http://www.ciba.com
Pfizer	4	3	x					http://www.pfizer.com
Pharmacia Upjohn	12	8	x					http://www.pnu.com
AETNA	6	5		x				http://www.aetna.com
AFLAC	1	1		x				http://www.aflac.com
BCBS	15	7		x				http://www.bcbs.com
CIGNA	8	5		x				http://www.cigna.com
eHealthInsurance	9	8		x				http://www.ehealthinsurance.com
Kaiser Permanente	5	1		x				http://www.kaiserpermanente.org
OnlineHealthPlan	8	9		x				http://www.onlinehealthplan.com
CornerDrugstore	17	9			x			http://www.cornerdrugstore.com
DestinationRX	17	18			x			http://www.destinationrx.com
Drugstore	17	14			x			http://www.drugstore.com
Eckerd	9	6			x			http://www.eckerd.com
HealthAllies	13	6			x			http://www.healthallies.com
HealthCentral	15	12			x			http://www.healthcentral.com
iVillage	23	19			x			http://www.ivillage.com
PrescriptionOnline	10	4			x			https://www.prescriptiononline.com
PrescribtionByMail	11	7			x			http://www.prescriptionbymail.com
WebRX	18	7			x			http://www.webrx.com
Nat. Inst. of Health	5	11				x		http://www.nih.gov
Centers for Disease Control/Prevention	7	9				x		http://www.cdc.gov
Breast Cancer	4	5				x		http://www.thebreastcancersite.com
AIDS Treatments	5	5				x		http://www.aids.org
Am Cancer Society	24	22				x		http://www.cancer.org
Am Diabetes Ass.	14	20				x		http://www.diabetes.org
Health Finder	9	10					x	http://www.healthfinder.gov
Merck-Medco	40	21					x	http://www.merck-medco.com
WellMed Tools	13	21					x	http://www.merck-medco.com
MyHealth Tool	43	22					x	http://www.merck-medco.com
WellMed	33	23					x	http://www.wellmed.com
WebMD Health	48	39					x	http://www.webmd.com
WebMd Practice	25	29					x	http://www.webmd.com
DrKoop	25	19					x	http://www.drkoop.com
MedScape	52	43					x	http://www.medscape.com
HealthScout	10	16					x	http://www.healthscout.com
Total	612	490	6	7	10	6	10	Total

If the Web site had more than one privacy policy available, each privacy policy is analyzed separately, for example, Merck-Medco had three different privacy policies available depending on which functions of the Web site were being used.

Item frequencies ("hits") in the protective and vulnerability categories are presented in Table 4. Figure 6 provides the scatter image of protective and vulnerability item hits per each studied Web site. [57]

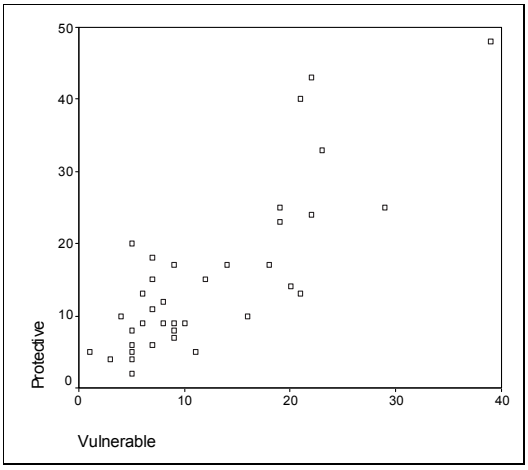

Figure 6: Scatter Images of Protective / Vulnerability Item Hits per Web Site.

Most of the Web sites are chosen very randomly, however, some were chosen carefully. For example, many health Web sites have been mentioned so far in this dissertation, and they are included in the sample as presented in Table 4. The following presents the same chosen Web sites in more detail.

Some of the most popular health Web sites are in the marketing and publishing business. In other words, they provide people with information about general fitness and nutrition, medical conditions, and treatment options. Some offer a broad range of information (classified as a general health site, e.g. DrKoop), while others specialize in a certain drug or medical condition (classified as a medical institute[58], e.g. Centers for Disease and Prevention).

[57] Two extreme observations AFLAC and MedScape were dropped outside of the analyses for validity reasons.

[58] Disease-specific sites and medical institutes were merged as Medical Institutes for reasons of analysis.

Some sites offer additional services that require users to provide personal information to the site. Many Web sites offer a "*health assessment*" feature where users may enter all sorts of information from height and weight to drug and alcohol use (e.g. MyHealthTool). The personal health information that consumers provide to many of these sites (e.g., through self-screening questionnaires or registration for email reminders) will not be protected by the privacy regulation. They do not have an offline existence where they engage in covered activities like treating patients. They only furnish health information – they do not provide "health care", as it is defined in the federal regulation[59].

Two Web sites, Centers for Disease and Prevention and Healthfinder, were chosen because they are on the Medical Library Association's Top Ten list of Most Useful Consumer Health Web Sites. Centers for Disease and Prevention, which is an agency of the Department of Health and Human Services, is dedicated to promoting "*health and quality of life by preventing and controlling disease, injury, and disability*." Of special interest to the consumer are the resources about diseases, conditions, and other special topics. Healthfinder is wide gateway consumer health information Web site. Menu lists on its home page provide links to online journals, medical dictionaries, minority health, and prevention and self-care.

In a national survey, commonly named illnesses included cancer and diabetes (Fox and Rainie, 2002). Therefore, one cancer and one diabetes Web site were chosen. One of those selected was MLA's recommended Diabetes Web Sites: American Diabetes Association. The American Diabetes Association is the leading non-profit health organization dedicated to diabetes. The mission of the organization is "*to prevent and cure diabetes and to improve the lives of all people affected by diabetes*." The site contains basic information about diabetes, such as healthy living choices, insulin reactions, exercise, and diet. Other features include diabetes in the news, online shopping, ADA-sponsored events, and a section for health care professionals. The American Cancer Society supports education and research in cancer prevention, diagnosis, detection, and treatment. Its Web site provides news, information on types of cancer, patient services, treatment options, a section on children with cancer and living with cancer, and cancer statistics.

Many commercial Web Sites were chosen, for example, Merck-Medco was chosen because it provides a wide category of different health care activities. Additionally, it manages prescriptions for 65 million Americans and has sold

[59] Privacy rule, § 160.103, available at http://www.hhs.gov/ocr/regtext.html

$1 billion worth of prescription drugs since its Internet pharmacy started three years ago (Schwab, 2001).

What do we know about .com health sites? Commercial sites may represent a specific company or be sponsored by company using the Web for commercial reasons – to sell products. At the same time, many commercial Web sites have valuable and credible information. The site should fully disclose the sponsor of the site, including the identities of commercial and non-commercial organizations that have contributed funding, services, or material to the site.

4.1.5 Method Assessment

The methodology employed in many empirical studies of business ethics, public sector ethics, and ethical decision-making has attracted criticism regarding respondent bias, lack of attention to theory, and failure to address validity (Cowton, 1998a). Content analysis, however, allows privacy policies to be analyzed in a transparent and reproducible manner, which is discussed in this section. Secondary sources can provide unobtrusive access when examining sensitive situations, and may reduce distortion due to imperfect recall and social desirability bias.

Theoretical sensitivity represents an important creative aspect of the used method. The core value framework of privacy, the balanced privacy framework, and the balanced privacy model enable an analyst to see privacy policy in a theoretical way.

Content analysis is a technique derived from data that has been systematically gathered, analyzed, and measured. A well-defined sampling design and system of categories and adequacy of operational definitions are all necessary to obtain valid results from content analysis (Berelson, 1952: Kolbe and Burnett, 1991). This section discusses how validity, consistency, and reliability issues were considered under the study.

4.1.5.1 Advantages and Limitations of Secondary Data

Empirical studies in business ethics often rely on self-reported data. Randall and Gibson (1990) reviewed 94 published empirical studies of ethical behavior and beliefs in organizations and found that self-report data was used in almost 90% of the studies. In another review of the empirical literature, Ford and

Richardson (1994) list 46 published studies of ethical decision-making. Over 95% of these relied on questionnaires, open-ended questions, interviews, or the subject's response to a scenario or vignette. Research methods texts generally adopt the position that secondary data is "*mere substitutes for 'better', but more expensive, primary data*" (Cowton, 1998b, p. 430), with particular concern being expressed that the researcher is unable to exercise any control over their generation. However, in certain uses, including some empirical studies in business ethics, it can be argued that secondary data actually has a number of advantages over primary sources. Gwartney, Fessenden and Landt (2002, p. 56) point out that content analysis of publicly available existing data and archives can be effective evaluation tools for five reasons. First, using existing data sources saves money and time, rather than spending limited resources on collecting original data. Second, these data sources represent participants' and constituents' own words, enhancing data validity. Third, such data can be gathered unobtrusively, avoiding biases introduced by survey instruments, interviewers' demeanor, or the presence of recording equipment. Fourth, such data are readily accessible over long periods, allowing relatively easy analysis to both long- and short-term outcomes. Fifth, by carefully reviewing such materials, researchers may operationalize those intangible and difficult concepts needed to understand such long-tem conflict resolution outcomes as leadership, motivation, collaboration, and interaction.

"*The unobtrusive access that they can present may help in reducing both social desirability response bias and the reluctance to respond to explicit ethical questions*" (Harris, 2001, p. 193). And "*virtually every empirical inquiry of issues relevant to applied business ethics involves the asking of questions that are sensitive, embarrassing, threatening, stigmatizing, or incriminating*" (Dalton and Metzger, 1992, p. 207). Much of the criticism regarding respondent bias relates to the heavy reliance placed on information obtained from individuals though interviews and questionnaires. Harris (2001, p. 191) points out that responses to questionnaires and interviews may be influenced by the subject's view of what the researcher might want to hear, by reluctance to talk about sensitive ethical issues, and by imperfect recall. Furthermore, since the early 1950s researchers in organizational sciences have expressed concern that the "*tendency of individuals to deny socially undesirable traits to admit to socially desirable ones*" may impair empirical studies based on questionnaires which require respondents to report on their own behavior or attitudes (Randall and Fernandes, 1991, p. 805). A further bias is introduced if some individuals decline to be interviewed and the

response patterns of respondents differ from those of non-respondents. This non-response bias would further increase the likelihood of and overall bias in the results (Cowton, 1998a).

Given these difficulties with primary data, Christopher Cowton concludes that "*secondary data may have attributes which render them highly attractive when compared to interview and questionnaire results*", drawing particular attention to the unobtrusive access available when dealing with sensitive situations (1998b, p. 432). This supports the earlier view of Dalton and Metzger that "*non-observational, non-reactive measures"*, including the examination of archival sources, are particularly appropriate for the collection of data in such circumstances (1992, p. 208). As "*managers are not likely to allow their 'ethics' to be observed or measured*" (Trevino, 1986, p. 601) and they may find it threatening "*to report honestly about their own cheating behaviour*" (Robertson, 1993, p. 588), there is the potential for distortion when interviewing individuals about their recollection of ethical behavior or about their intended behavior (Harris, 2001, p. 192).

There are, however, some limitations of secondary data in the setting of e-commerce privacy practices. The used technique does not reveal those privacy matters that are not expressed in privacy policy statements. Research from the outside organization using online privacy policies overlooks some features that may render the study results epistemologically worthless, for example, it does not reveal the number of security and privacy incidents in the company. The numbers and categories of possible incidents could be used as an effective metrics. The more developed metrics could include many different concepts, for example, the definitions of employee action in specific settings, the employee interest (motives, incentives, purposes), and the historical matters and experiences. It would be an advantage if the used method also contained the "*self-regulation*" perspective from the inside, because Thompson (1999; 2001, p. 16) argues that it may not always be appropriate to presume that measuring the probability of an unwanted outcome is an appropriate way of responding to the judgment that a particular activity is risky. Kreps (1997) asserts that providing extrinsic rules and incentives for workers can even be counterproductive. It may destroy the workers' intrinsic motivation, leading to a lessened level of quality-weighted effort. Many principles, for example, the justification of exceptions and core value considerations, entail that the privacy issue on the Internet be a very quality-dependent issue. This is not to say that intrinsic motivation is always superior to extrinsic rules and incentives, but it could be a new interesting point to study in the topic. Such shortcomings can be overcome by inquiry from the inside organization

(Evered and Louis, 1981). Ethnomethodology and anthropology methods represent systematic approaches to this mode of inquiry.

Management of the users' privacy protection can be very effective using the self-regulation perspective from the inside, but the main problem is how customers are able to realize the actual privacy situation and take reasoned actions based on that (inside knowledge). Secondly, these sensitive issues are very difficult to discover as discussed, and thirdly, a common criticism of the field study method involves four main types of threats: observer-caused effects, observed bias, data access limitations, and complexities and limitations of the human mind (McKinnon, 1988). If we study possible privacy incidents in the company, all of those threats seem to be noteworthy and even paramount.

The study focused on information-rich business segments in the health care industry where consumer vulnerability is exceptionally high due to the sensitive nature of information collected at these Web sites. In such a situation, it is important to help customers evaluate and make decisions between practices that protect their privacy and practices that may introduce potential vulnerabilities, and therefore, two major privacy item categories are used in which privacy statement are broadly categorized as either privacy protective items or privacy vulnerability items. There were, however, some interpretative problems of the categorization, because items were not clearly separated in Web site privacy policies. The core value framework of privacy, the balanced privacy framework, and the balanced privacy model item coupled with the categories provides a basis for identifying conflicting statements within a privacy policy, but some privacy invasions are benign or can at least can be interpreted that way by some customers. The problem is that what one customer considers a privacy invasion (vulnerability items) may be a valued feature or service to another consumer. Other categories presented later (visibility and modularity) have the same minor problems. Attempts have been made to manage interpretive problems by carefully considering each item's actual intent; its properties.

Critics might argue that items and categorizations and other ways of looking at and capturing the privacy practices under the study were screened out. Of course, anticipatory data reduction did occur. This should not cause undue concern. First, the presented frameworks and models, the coding schemas, and the study questions are explorative. Next, it would have been hidebound to ignore the value of existing empirical and conceptual work as an orienting frame. Additionally, personal experience represents one source of theoretical sensitivity in this study. This knowledge, even if implicit, was

taken into the research situation and it helped the researchers understand e-health actions and privacy policy statements. As an example, the experience of having searched health care information on the Internet or having ordered something using the Internet makes one sensitive to what it means to experience privacy, communication practices, trust, and efficiency. This sensitivity is very subjective, and therefore one must be careful not to assume that everyone else's experience has been similar to that of a researcher. However, Harris (2001, p. 201) points out that the use of content analysis can help to constrain the researcher faced with the temptation to arrive at more extensive conclusions than the data would support.

The research methods, such as content analysis, used in dealing with secondary data are more easily amenable to replication and to validity and reliability checks than some methods used to collect primary data in social settings (Frankfort-Nachmias and Nachmias, 1996), and Hakim suggests that the use of secondary data "*forces the researcher to think more closely about the theoretical aims and substantive issues of the study*" (1982, p. 16). The more sensitive a researcher is to the theoretical relevance of certain items, the more likely the researcher is to recognize indicators of them in the data. This sensitivity usually grows throughout the duration of a research project, and helps the researcher decide what items to look for, where the researcher might find evidence of them, and how the researcher can recognize them as indicators (Strauss and Corbin, 1990, p. 180).

4.1.5.2 Validity, Consistency and Reliability

Four sources of knowledge that might be utilized to develop and justify analytical constructs and which may have to be used in validating any analytical procedure are knowledge of past success with similar constructs or situations, representative interpreters and experts, established theories of dependency among the data, and experiences with the context of the data (Krippendorff, 1980). The successful past use of content analysis and experiences with the context of the data are reported in the preceding sections. In addition, direct feedback has helped to develop the presented privacy analyses and frameworks.[60]

[60] Privacy experts in North Carolina State University and in Georgia Institute of Technology have commented on the presented analytical constructs, and the feedback from the Eighth Americas Conference on Information Systems (AMCIS 2002), Dallas, Texas; and from the Second Symposium in Requirements Engineering for Information Security, Raleigh, NC, USA, October, 2002; and from

Although the purpose of many business ethics studies will not be to use the data collected by content analysis to construct a precise scientific theory, a number of steps can be taken *"to provide evidence that systematic and spurious errors occur infrequently"* (Janis, 1965, p. 81). An explicit procedure for content analysis, like other research instruments, is "*said to have validity if it measures what it purports to measure; it has reliability if it gives the same result consistently*" (Hagood, 1941, p. 219). The objective is that another researcher would end with the same findings and conclusions if he were following exactly the same procedures described in the research report. External validity and generalization describes the extent to which the study's findings can be generalized to other samples (Yin, 1991).

Krippendorff, whose extensive coverage of validity in content analysis (1980), identifies many aspects of validity including some aspects of reliability. *"Sampling validity"* is concerned with any sampling that occurred in the selection of the texts to be examined and in the selection of the samples to be used for the pilot study and for the check coding exercise. In this dissertation, sampling validity was discussed when the pilot study and the analyzed Web sites were presented. *"Semantic validity"* is the extent to which privacy policy statements placed in the same category have similar meanings and relate to the category in a similar fashion (Krippendorff, 1980, p. 164). *"Construct validity"* refers to the establishment of correct operational measures for the concepts being studied (Yin, 1991). Tests of *"construct validity"* can only offer "*a weight of evidence that your measure either does or doesn't tap the quality you want it to measure, without providing definite proof"* (Babbie, 1995, p. 128). One further type of validity, not included in the Krippendorff typology, is *"face validity"*. The extent that a category appears to measure the construct that it is intended to measure (Weber, 1990; Babbie, 1995).

Calculation and reporting of reliabilities are essential to content analysis, and reliabilities for individual items are better than pooling results (Kolbe and Burnett, 1991). The importance of the reliability of a research method "*rests on the assurance that it provides that the data are obtained independent of the measuring event, instrument or person. Reliable data, by definition, are data that remain constant throughout variations in the measuring process*" (Kaplan and Goldsen, 1965, p. 83). There are three types of reliability in the Krippendorff categorization: reproducibility, stability, and accuracy. *"The*

---

the first Combining Views from IS and Service Research Seminar, Turku. Finland, June, 2003, has helped to develop the presented privacy frameworks.

reproducibility reliability" of the coding is assessed by having a sample of items coded by a number of independent coders and comparing the results. *"Stability"* is the degree to which the results of content categorization and coding remain consistent over time. *"Accuracy reliability"* is a measure of the extent "*to which a process functionally conforms to a known standard, or yields what it is designed to yield*", but as the standards against which the coding of texts into categories could be assessed are rarely available, Krippendorff concludes that "*it is largely unrealistic to insist on*" this reliability criterion (1980, p. 132). Harris (2001, p. 195) points out that accuracy reliability "*may not just be unrealistic, but also unnecessary*".

Consistency in this study means gathering data systematically on each category. In order to answer the study questions, it was important to uncover all significant, important and interesting items, along with the most relevant categories and their properties, and this is why so many health privacy policies were chosen and analyzed. For this report, every effort was made to ensure that each of the 39 privacy policies in the sample was evaluated using the same categories, coding schemes, and theoretical knowledge. The criticism by quantitative researchers is that qualitative data collection yields data that is non-comparable (Strauss and Corbin, 1990, p. 191). Privacy policy documents that constitute the data are comparable because all studied privacy policies were reviewed in the spring of 2003 using the same knowledge and metrics.

The research team began phase 2 (see Table 1) with conceptual consensus among the research team with various scientific persuasions (technology, social, cultural, health care, and business), and then allowed each discipline to inform the others about more compelling or promising ways to look at the phenomena all were studying. This phase added theoretical sensitivity, but also objectivism for the study. It wasn't easy to make creative use of one's knowledge and experience while at the same time holding on to the reality of a phenomenon, rather than just thinking imaginatively about it (Strauss and Corbin, 1990, p. 44). While many of the analytical techniques that one uses to develop theoretical sensitivity are creative and imaginative in character (Strauss and Corbin, 1990, p. 47), it is important to keep a balance between that which is created by the researcher and the reality. To assist researchers, Strauss and Corbin (1990, p. 47) offer the following suggestions.

- Periodically step back and ask: What is going on here? Does what I think I see fit the reality of the data?
- Maintain an attitude of skepticism. All theoretical explanations, categories, hypotheses, and questions about the data, whether they come directly or indirectly from the comparisons, the literature, or

from experience, should be regarded as provisional. They always need to be checked out, played against the actual data, and never accepted as fact. Categories derived from the research literature (variables identified in previous studies) are always context-specific.

- Follow the research procedures. The data collection and analytic procedures are designed to give rigor to a study. At the same time they help you to break through biases, and lead you to examine at least some of your assumptions that might otherwise affect an unrealistic reading of the data.

All of these were used during the study process. The study was designed to be redesigned as a function of emerging concepts, thereby remaining data-sensitive and non-frozen. The content analysis process allowed for each significant variation in privacy policy statement content to be coded in a distinct and consistent manner. Item identification and item reduction schemes were used. Unambiguous category coding schemes were used because content analysis requires not only a set of categories that are "*independent, exhaustive and mutually exclusive*" (Sarantakos, 1993, p. 212), but also the rigorous use of a clear set of coding guidelines (Strauss, 1987). Coding represented the operations by which privacy policies were broken down and put back together in new ways. Item identification, item reduction, and categorizing using coding schemes were the central processes by which these explorative study results were built from data. One of the coding rules adopted was to specify that any item be assigned to only one category in a given category scheme; the one where it fit best. Thus, single categorization was used rather than multiple categorizations in a one category scheme. This reduces the opportunity for the coder to seek multiple "hits" for a single item.

Statistical analysis can be used to evaluate the aspects of validity, consistency, and reliability of this study. A number of different measures[61] can be used to express the extent of agreement achieved among coders regarding the assignment of items to categories. "*One is the proportion of all category assignments in which there is a perfect match among all coders, called '% match'* " (Harris, 2001, p. 200). When there are more than two coders, there may be cases of majority agreement as well as unanimous agreement. The

[61] It is possible to calculate reliability for content analysis items by using, for example, the Perreault and Leigh reliability index: $I_r = \{[(F0/N)-(1/k)][k/(k-1)]\}0.5$, for $F0/N>1/k$, where F0 is the observed frequency of agreement between coders, N is the total number of judgments, and k is the number of categories. This index accounts for coder change agreement; the number of categories used, and is sensitive to coding weaknesses. Reliability scores can range from 0 to 1, with higher scores indicating greater inter-coder agreement. See William D. Perreault and Laurence E. Leight (1989).

proportion of all codings where a majority of coders agree is called the "*reliability coefficient*". Some agreements may have arisen by chance, and the "*agreement coefficient"* compares the agreement achieved by the coders with the level of agreement that might be observed had chance been employed as the basis for coding. It also takes into account sample size, the complexity of the data, and the number of coders, and Krippendorff considers it to be most convincing measure available (1980).

In this study only the %matches were calculated on the basis of mature deliberation. In order to establish the reliability of the coding on which the empirical study is based, however, substantial check coding activities were undertaken. This involved three researchers, a test sample of a privacy policy, specific training, and statistical analysis of the results. In order to test item identification and item reduction schemes the author assessed one EU directive, one EU recommendation, and the privacy policy of URAC. After this amendment of theoretical sensitivity phase, two reliability measures – reproducibility and stability – were assessed, along with a check of face validity. The previously analyzed 23 privacy policies were chosen for the check coding, selected on the basis that reliability testing "*is served best by a stratified sampling design that assumes that all categories of analysis, all decisions specified in the forms of instructions are indeed represented in the reliability data regardless of how frequently they may occur in the actual data*" (Krippendorff, 1980, p. 146).

The presented empirical study included four phases, which are presented in Table 5. The first phase of the research was collaborative in nature. It was performed as a pilot study by two researchers and one graduate student (the author was not involved). It consisted of the 23 health care Web sites' privacy policies. Privacy policies were chosen in three health care segments: pharmaceuticals, health insurance, and online drugstores. The study led to 134 different items and 405 hits. It resulted in a draft version of the data and an evaluation instrument. The author joined in the research team (and the student departed) in the summer of 2001.

To test the reproducibility reliability, the author analyzed the full privacy policies to count hits or non-hits of items under each of the major – protective and vulnerability – categories of the framework. The second phase resulted in a reliability score of almost 100% (one hit dropped out). When there were some disagreements during the second phase, every result of the privacy policy analysis was discussed amongst the research team members until consensus was reached and the necessary definitional and procedural changes could be made. The research team found it essential to elaborate and obtain

agreement among the members in the second phase concerning basic instrumentation with two major categories. As a result of the second phase, the Excel spreadsheet file that constituted the data collection form,, the dictionary, and the major coding schemes were modified to provide additional clarity. Therefore, an acceptable level of inter-judge reliability was established for the privacy policy evaluation process, and a data set was created based on the consensus of the research team.

Using those re-analyzed privacy policies, the author determined new categories to be used, and so initial visibility and modularity category coding schemes were generated. When the author was faced with an interpretive problem concerning those new category coding schemes, the whole team reviewed and evaluated the privacy policy statement. A majority rules policy was used to determine the final coding in those cases.

The third phase consisted of the privacy policies of the 16 health care Web sites. Privacy policies were chosen in two health care segments: medical institutes/disease-specific services and general health information services. The phase resulted in 226 different items and 672 hits. In a study where all the coding is done by the individual researcher, the reproducibility reliability cannot be calculated, which was the case concerning the 16 privacy policies in Phase 3 and Phase 4. However, the stability reliability was tested. The author coded a sample of the original 23 Web sites again in the spring of 2003 (Phase 4), which resulted in a stability reliability score of over 90%. Increased theoretical sensitivity yielded the information that some new items and hits (the original 405 item hits increased to 430 item hits) were found by the author.

Table 5: Modularity Category Items and Hits.

Phase	***Timetable***	***Web sites***	***Items***	***Hits/23***	***Hits/16***	***Total Hits***
1	Spring 2001	23/3 segments	134	405	-	405
2	Fall 2001	23/3 segments	134	404	-	404
3	Fall 2002	16/2 segments	226	-	672	672
4	Spring 2003	39/5 segments	226	430	672	1102

The lack of an effective tool was one of the disadvantages of the used method. All analysis phases of this study were done without support of any tool. "*Complex forms of content analysis require extensive human input*" (Franzosi, 1995, p. 157). While this may increase the time and personal effort required for the empirical study, reliability is improved by the combination of

hand coding with the phrase as the unit of analysis (Insch, Moore and Murphy, 1997). The results for reliability demonstrate that the category schemes of this study were clearly defined, and could be located in the privacy policy statements with little ambiguity. There are only a few reported cases of a rigorous reliability check for empirical research in ethics, (Harris, 2001, p. 200), but the approximation obtained in the "privacy policy" study seems to be rather good when compared those where reliability results are reported (Janda, 1969; Allen, 1995; Howell and Higgins, 1990; Henningham, 1996; Jamal and Bowie, 1995; Harris, 2001).

4.1.5.3 Generalization

One sub-goal of this explorative study is the development of a "set of *propositions*" that yields valid and meaningful (i.e. not truistic) predictions about phenomena not yet observed (Friedman, 1953). The focus is upon the process of testing propositions in an inductive sense in accordance with the canons of scientific rigor.

In quantitative forms of research, sampling is based on selecting a portion of a population to represent the entire population to which one wants to generalize. Therefore, 39 health care Web sites have been chosen in five health care segments by providing sampling validity. Different segments allow wider applicability of the privacy frameworks, because more and different sets of concepts and conditions affecting privacy are uncovered.

The general rule in research is to sample until theoretical saturation of each category is reached. This means until no new or relevant data seem to emerge regarding a category; the category development is dense, insofar as all of the privacy elements are accounted for along with variation and process; and the relationships between categories are well-established and validated (Glaser, 1978, pp. 124-126; Glaser and Strauss, 1967, pp. 61-62, 111-112). Naturally, the more privacy policies obtained, the more evidence and items will accumulate as seen in Table 5, the more variations will be found, and the greater density will be achieved. But we should note that there is a practical limit to the number of privacy policies, categories, and variables that any study can take into account. Thus, the overriding consideration is the representativeness of that sample, or how much it resembles that population in terms of specified characteristics. In reality, one can never be certain that a sample is completely representative. In quantitative research, however, certain procedures and statistical measures help to minimize or control the problem

(Strauss and Corbin, 1990, p. 190). In this study, these issues are also handled and accounted for. The propositions are tested using analysis of variance (ANOVA) and t-test paired observations using the SPSS program (version 10.1). The number of studied Web sites is 39, and the scale reliabilities of the study measures range between 0.1 and 0.5. The numbers of analyzed privacy policies and reliabilities are deemed acceptable for exploratory studies (Morgan and Hunt, 1994; Anderson, Sweeney and Williams, 1993). Technically all analyses were valid and they are documented in a way that allows for repetition.

External validity and generalization describes the extent to which the study's findings can be generalized to other samples and therefore Internet privacy policies for services in the five health care segments that were analyzed: pharmaceuticals, health insurance, online drugstores, medical institutes/disease-specific services, and general health information services. The results reported here present evidence on the nature of relationships between customers and health providers found in the privacy policies. The results of these kinds of analyses are expected to provide additional benefits to policy makers and consumers by providing more objective criteria for evaluating a Web site's privacy practices. The number of the studied Web sites and the scale reliabilities of the study measures give some evidence for generalization, but there are also many limitations to consider. In terms of making generalizations to a larger population, this study is not attempting to generalize as such, but to provide aspects to consider. This means that this explorative study applies to these situations and circumstances but no others.

When conditions change, then the study formulation will have to change to meet those new conditions. The health care sector and services in these markets are clearly differently organized and function differently among various countries, thus the results of this study are not valid outside the U.S. For example, the legal category is expected to present different results when applying the framework to international Web sites that are not focused in the U.S. The European directives tend to protect and secure the privacy of the user and not threaten it. Furthermore, it seems that business and health care-related Internet services have different requirements concerning privacy. Therefore, future studies need to re-examine and define the measures. These issues are discussed in more detail in Section 5.

When developing a formal theory, a researcher must study privacy issues in several types of situations. Note that even if the sample were broadly collected, for example, the privacy policies of health care organizations chosen randomly from different health care segments, it still has elements only for a

substantive theory (Strauss and Corbin, 1990, p. 174). The error sometimes made by researchers is that they think they can make the leap from substantive to formal theory because they have generalized to different types of situations from a phenomenon studied in only one situation. However cautiously a researcher may suggest the wider applicability of his or her substantive theory, this cannot be done with any assurance unless these other situations have also been studied. This is, indeed, how a substantive theory can be properly developed into a formal theory (Glaser, 1978, p. 142-157). In short, it is not the level of conditions that makes the difference between substantive and formal theories, but the variety of situations studied.

4.1.6 Conclusion

Diana Robertson (1993) suggests the need to establish validity for the future direction of business ethics research. She also draws attention to the weak link that exists between empirical research and the generation of theory. But as qualitative researchers are discovering that procedures for protecting reliability and heightening validity can be as rigorous as the canons of classical test theory (see Guba and Lincoln, 1981; Huberman and Crandall, 1981), the disciplined application of content analysis to privacy practices from health Web site privacy policies may go some way toward addressing those concerns with respondent bias, lack of attention to theoretical sensitivity, and failure to address validity.

The use of content analysis for studying privacy policies brought additional benefits to the overall research activity. It allows an assessment of the validity and reliability of the empirical research to be made, and meant that the categorization process and the basis of categorization were clearly specified and open to scrutiny. The data collection phase was addressed carefully by specifying the boundaries of data collection, and by standardizing the items using item reduction and a category coding scheme to allow the production of reasonably comparable data sets across 39 Web sites. Several items were used to measure privacy practices to understand how companies employed privacy policies for expressing privacy practices. The main point of emphasis is that iterative procedures are also needed: data are collected, coded, analyzed, and the new data collected as a function of that analysis – until, after several such phases, the final analyzed data is plausible, internally consistent, and verified by recourse to multiple sources of theoretical sensitivity. Some categories were arrived at inductively and others came about as a result of deductive

thinking during the analysis. Testing is a crucially important and integral part of the used method. It was built into each step of the process. Though not testing in a statistical sense, the author constantly compared propositions against reality (the data), made modifications, and tested again.

Furthermore, by requiring the derivation of the categories, properties, and coding schemes from a theoretical sensitivity, the rigorous application of the eight-step content analysis procedure may encourage researchers to develop closer links between the theoretical and empirical components of the research, thus responding to the call from Robertson and others for greater attention to theory. Comparing privacy policies using numbers of presented category items is an innovative and effective analysis method that enables us to provide useful guidance to the customers and organizations. Content analysis is considered a reputable and widely utilized tool for conducting objective, systematic, and quantitative analysis of communication contents (Berelson, 1952; Kassarjian, 1977; O'Connor and Adams, 1999). There is no evidence of what Weaver and Trevino call the "*parallel approach*" to business ethics research, where normative inquiry becomes "*too abstract, too idealistic, to be of any practical value*" by avoiding any contact with empirical research (1994, p. 132).

4.2 Communications Practices of Privacy Matters

This section discusses what communications practices of privacy matters are found in the analyzed health care privacy policies. To assess what communication practices of privacy matters are found in health care privacy policies, sample sites were analyzed using the content analysis to determine the existence of practice. The samples illustrate how companies assist customers as they try to gain control over privacy policy revisions at the Web sites they visit. One of the interests is how online companies treated information that was gathered before the change of privacy policy. Other communication practices of privacy matters are discussed in Section 4.4, when privacy seal programs are presented.

4.2.1 Demands

One problem of sufficiently protecting customer privacy is that the privacy policy that is appropriate and accurate today may not be that way for long. The entire Internet infrastructure is continually developing, and therefore the iteration of privacy policy adjustments is needed. This is partly a technical issue, because technology rapidly introduces new possibilities, but it also has many other consequences, as discussed in Section 3. Technical improvements enable more functional and complex electronic commerce applications´, and technical solutions offer possibilities to strengthen privacy and security issues. Consequently, these solutions and improvements can threaten or support ethical objectives. When new technologies are adopted, an organization's security policy and privacy policy must be revisited and oftentimes revised to respond to policy conflicts introduced by these new technologies.

Internet services should be designed so that all protection of privacy information should be easily understandable by everybody. A key characteristic of the Internet is that users are totally in control of which sites they visit and how long they stay. Therefore, more and more companies are providing features that facilitate site navigation for prospective customers. As mentioned earlier, site security and privacy issues continue to be a major concern for Internet users. However, not all the evaluated health care Web sites were making an effort to alleviate this concern for visitors. Basic site navigational tools like an internal search engine for privacy policies were not found on most of the health care Web sites. Suppose that customers are very highly informed about the structures and policy of the Internet service, including all possible threats and vulnerabilities. If that is the case, customers can select the Internet service on the basis of very detailed chains of reasoning and choose the Service-on-Demand (S_y) and the Privacy-on-Demand (P_x) accordingly, as the balanced privacy model suggests.

Keeping the privacy policy as up-to-date as possible should be the important theme for the whole organization. It is important that consumers are being notified and made aware of an organization's new privacy policy. The balanced privacy framework asserts that consumers should be notified and/or made aware of an organization's information practices before any information is actually collected from them. When applying the balanced privacy model to changed situations, we should have an open debate and dialogue regarding which data subjects would first be informed of the existence of the new practice. Customers would also be informed that, currently, data about them collected for one purpose can also be used in ways that they probably had not

explicitly authorized. Customers need to be aware of current changes in an organization's information practices before any new information is collected from them or before their data is used in an undesirable manner. When an organization modifies its privacy policy, there will most likely be conflicts between the old and new policies. One trustworthy aspect of privacy policy is that the intended use of any gathered information is fully declared. Trust ís defined as the expectation that an organization will not engage in opportunistic behavior. In order to avoid opportunism, information that was collected under the previous privacy policy should not be used pursuant to the new privacy policy without first obtaining user consent. The interactivity features of the Internet give many possibilities for communication practices of privacy matters.

For example, Internet companies should ordinarily secure each customer the right of determining to what extent his personal information shall be communicated to others. Generally online privacy policies contain provisions for sharing customer information with law enforcement agencies in the event of a criminal investigation or suspected illegal activity (see Privacy Policy Statement #4 and Privacy Policy Statement #5). Nevertheless, some companies that have been cooperating with authorities investigating the September 11th attacks have been reviewing their actions for possible privacy violations. A key issue, privacy advocates say, has come from companies that worry they may have gone too far in handing over complete databases to law enforcement in the immediate aftershocks of the attacks without requiring a court order or a subpoena (Olsen, 2001). For example, Ray Everett-Church[62], pointed out that,

> *"I've never seen a privacy policy that says we will make all of our records available to authorities in a case of national emergency, and I think as a result of this, you're probably going to see companies adjust their privacy policies to take this into consideration"*
> *(Olsen, 2001).*

The management of privacy policy should successfully anticipate the environmental shocks[63]. Even the most anticipated person may on occasion recognize that the organization is being asked to deal with environments that

---

[62] Senior privacy strategist at the Los Angeles-based ePrivacy Group.

[63] The situation after September 11th is discussed in more detail in an article by Järvinen O.P. (2003) Revision of Privacy Policy: Five Perspectives and ONION-model. People and Computers: Twenty-one Ways of Looking at Information Systems. (ed. Järvi, T. & Reijonen P.) TUCS General Publication, No 26, June 2003, pp. 167 – 184.

are full of surprises. The justification of exception principle is a convenient principle for exceptional occurrences, but there is also the threat of overreaction.

Figure 7 illustrates the different privacy communication practices found in 39 health care Web sites privacy policies.

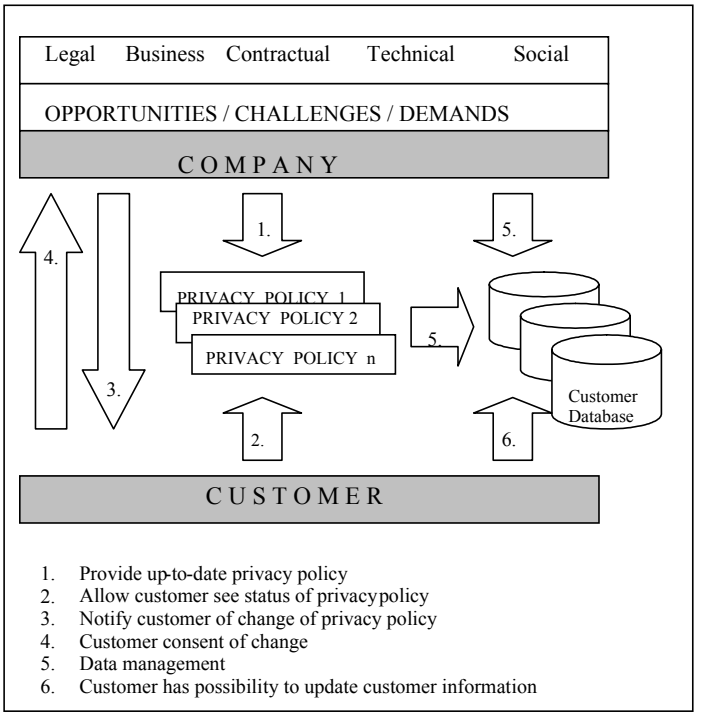

Figure 7: Privacy Communication Practices.

Health providers are subject to several different influences, for example, legal constraints constitute demands, business situations generate challenges, technical improvements allow opportunities, and contractual and social issues set requirements, as discussed in the preceding sections. Each of these demands flexibility on behalf of the organization. The iterative process of maintaining an up-to-date privacy policy is therefore needed.

4.2.2 Up-to-Date Privacy Policy

The demand to keep a Web site's privacy policy accurate in such a changing and evolving environment implies that the organization is capable of

modifying its privacy policy when necessary (arrow 1, Figure 7). Consider Privacy Policy Statement #8 taken from the Merck-Medco privacy policy:

Privacy Policy Statement #8:

> *Merck-Medco reserves the right at its discretion to change, modify, add or remove portions of this policy, or any of its supplemental policies, at any time.*

Of the 39 organizations included in the privacy policy analysis, only 20 of those clearly stated that they had reserved the right to change their Web site's privacy policy at any time. The other 19 did not express anything about the matter, which suggests customer privacy is not a fundamental priority for those organizations. Consider a conscientious customer who reads the Bayer privacy policy (one of the 19 previously mentioned) before continuing to visit the Web site or engaging in online transactions with the Web site. If the customer is satisfied with his or her experience, then he/she will likely return to Bayer's Web site at a later date and will see no reason to re-read the privacy policy on subsequent visits. Given the dynamic nature of the Internet and its associated technologies, Bayer will most likely alter its data collection and management practices at some point. When that happens, Bayer is faced with two options: modify the Web site privacy policy without the customer realizing privacy practices have changed, or maintain the original privacy policy that now inaccurately reflects the Web site's privacy practices. Both options place the customer in a vulnerable position with respect to privacy.

The mechanism by which consumers are typically made aware of privacy practice changes is through the presence of an up-to-date privacy policy. The approach is illustrated by item I_{11}: `POST changes to privacy policy on Web site`, which was found in 18 privacy policies (arrow 1). It places the responsibility for learning about changes on the site's users, who presumably must revisit the site and read its policy carefully on a regular basis. Because it, however, provides the balanced privacy framework, it is categorized as a protective item.

Consider Privacy Policy Statement #9 taken from the iVillage privacy policy:

Privacy Policy Statement #9:

> *We encourage you to periodically review our Privacy Policy to be sure you are familiar with the most current version. This*

Policy will include the most recent date in which any revision has been made.

Many Web sites display the date of the last privacy revision/update as an indication of the reliability and time-sensitivity of privacy information. Over 50% of the Web sites in the sample offered this information. Twenty companies clearly stated the revision date of their privacy policy (arrow 2, Figure 7). When the revision date was provided, it was not displayed in a consistent manner from one Web site to another. Several Web sites required extensive searching to find either the revision date or to ensure that there was not a revision date available. Table 6 depicts where the revision date was placed.

Table 6: Location of the Revision Date.

Location	***Total***
At the top of the privacy policy	3 (15%)
In the middle of the privacy policy	2 (10%)
At the end of the privacy policy	14 (70%)
At the end and at the top of the privacy policy	1 (5%)
Total	20

Online users should begin the search process at the end of the privacy policy. If the revision date is provided, this will be the location over half the time. The problem is that the user does not know the situation in advance. If a date is not available, it requires much searching before the user can be sure that is the case.

The second mechanism is evident in ensuring that consumers are aware of privacy policy changes. It is illustrated by item I_{12}: `NOTIFY customer of changes to privacy policy`, which obligates the site to notify its users of changes to its policy (arrow 3, Figure 7). Eleven Web sites promised to send an email message to all registered users notifying them that the privacy policy had changed. When the Web site actively notifies the customer, such an item is categorized as a protective one as it supports the balanced privacy framework. A practice such as this is a protective feature that occurs with the user's awareness; therefore, it is part of the visible category.

The modification of a privacy policy can introduce vulnerability to a customer if the Web site does not express its revisions clearly.

Consider Privacy Policy Statement #10 taken from the WebMd Practice privacy policy:

Privacy Policy Statement #10:

> *We may change this Privacy Policy at any time by posting revisions to our site. Your use of the site constitutes acceptance of the provisions of this privacy policy and your continued usage after such changes are posted constitutes acceptance of each revised Privacy Policy.*

Such a policy could introduce vulnerability to the user. In this case, it is feasible for the customer to unknowingly give consent and approval (arrow 4, Figure 7). The practice works as the positive voluntary principle, but the problem comes into existence when the customer is not aware of that. These types of statement were found in five of the analyzed privacy policies. In these cases, the responsibility is left to the customer to read and understand the entire privacy policy at every visit.

The impacts of privacy policy revisions can have an effect on data collected after the change, as well as on data that was collected before the change. However, one positive approach is illustrated by Privacy Policy Statement #11 taken from the My Health Journal Tool privacy policy.

Privacy Policy Statement #11:

> *Before we make any other use of information that we collect through this tool in a manner that identifies the user by name or address, we will update this statement to describe that use. For any new use, we will only use information that is collected after this statement has been updated to describe that use.*

Although this mechanism requires the customer to review the privacy policy before every visit, the customer can be confident that the Web site is taking customer awareness seriously. This practice provides the balanced privacy framework. However, the balanced privacy model is not sufficiently provided, because it may provide insufficient and lean service function.

A different approach, yet still a positive one, is illustrated by Privacy Policy Statement #12 taken from the DrKoop privacy policy. It supports the balanced privacy model more sufficiently than the preceding example.

Privacy Policy Statement #12:

> *We will notify our users if we make significant changes to our privacy policy that may affect the use of health-related information, and we will obtain consent from consumers for new uses of that data.*

Some privacy policies stated clearly that data collected before policy revision would not be used in the new manner until obtaining user consent. Item I_{13}: `PREVENT new use of PII after change of privacy policy without consent`, was present in eight privacy policies. In addition, two privacy policies stated that they do not use old data in a new way in any case.

Allowing customers to provide or decline consent and managing privacy policy revisions requires more complex data management. One approach is illustrated by arrow 5 (Figure 7). As an example, consider Privacy Policy Statement #13 taken from DestinationRX.

Privacy Policy Statement #13:

> *If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify users by way of an email and wait for your consent. Users will have a choice as to whether or not we use their information in this different manner. We will use information in accordance with the privacy policy under which the information was collected.*

This kind of fair policy requires data management. Customer data must be labeled with additional information, such as the privacy policy version when consent was obtained. This policy gives the company the opportunity to use old knowledge and new information effectively but is also trustworthy as the balanced privacy model proposes. This policy provides customers with possibilities to choose the level of service and privacy, i.e. Privacy-on-Demand and Service-on-Demand functions accordingly.

Arrow 6 (Figure 7) illustrates the second approach, which targets the same concept. Consider Privacy Policy Statement #14 taken from CornerDrugstore:

Privacy Policy Statement #14:

> *Your use of the site constitutes acceptance of the provisions of this Privacy Policy. CornerDrugstore.com may change this privacy at any time. Registered users will be notified by email if there are substantive changes in this Privacy Policy. At that time, users will be given the opportunity to cancel their accounts, if they do not accept the privacy policy changes. If you do not agree to the terms of this Privacy Policy, or revised policy, please do not use the site. Reviewed August 2001.*

Using this tactic, the customer has the opportunity to manipulate his/her information. Data management is provided in such a way that all gathered data is complies with the latest privacy policy, but the user has the option to cancel older data if he/she does not accept the revised privacy policy. (Privacy Policy Statement #14 provides, thus, arrow 1, arrow 2, arrow 3, and arrow 4 accordingly).

According to the balanced privacy framework, Privacy Policy Statement #12, Privacy Policy Statement #13, and Privacy Policy Statement #14 include the clear presumption that customer informational privacy is a positive core value which is worth protecting. In particular, Privacy Policy Statement # 13 and Privacy Policy Statement #14 pursue the balanced privacy model.

Employing an interactive dialog by demanding or consenting, customers are able to change Privacy-on-Demand and Service-on-Demand functions. The practice makes privacy issues more exact to consumers, thus enabling them to choose privacy practices and make more informed decisions about privacy situations and what kind of service functions they prefer. If the company changes privacy situations without consent or demand by the customer, it is leaning toward opportunism or deficit electronic commerce business.

4.2.3 Discussion

The comparative strengths and weaknesses of these privacy policies could be elaborated upon, but people may not agree on exactly how to rank privacy policies. For example, some may believe that notification by email (Privacy Policy Statement #13) is worse than no email at all (Privacy Policy Statement #9), because email is not a secure media and there have been failures, as discussed in Section 1.1. In that case, Privacy Policy Statement #13 is worse

than Privacy Policy Statement #9. Some may believe that Privacy Policy Statement #9 creates risks because some misunderstanding about what is being changing could happen. In that case, Privacy Policy Statement #13 is better than Privacy Policy Statement #9. The balanced privacy framework and the balanced privacy model provide us with a set of principles with which to assess policies. From the customer's perspective, nobody would argue that no privacy policy at all or no clear privacy policy change practice is acceptable. Privacy Policy Statement #10 "*demands*" that customers periodically review their privacy policy to be sure customers are familiar with the most current version. It places, therefore, a tremendous burden on customers who want to act according to the negative voluntary principle. It does not directly reflect the principles presented in the balanced privacy model either.

Most would agree on the basis of the presented privacy framework that some privacy policies are acceptable and that some are better than others. Moreover, even when there is disagreement about the rankings, the disagreements may have as much to do with factual matters as with value differences. As a matter of fact, could the new use of personal information cause more damage than email notification, and as a matter of fact, do misunderstandings about what is or is not changed occur? The situation is equal to evaluation of the whole privacy policy. Some privacy policies mean vulnerability to customers and some practices are very protective. There are disagreements about the rankings of some in the middle. Often reasons can be given about why some are better than others. Similarly, some privacy polices and practices for using customers' information are ethically unacceptable whereas others are not. People may have different rankings, but these rankings, assuming the customer privacy point of view, will have a significant positive correlation. Moreover, people can give reasons why some privacy policies statements are better than others. The core value framework of privacy, the balanced privacy framework, and the balanced privacy model provide a set of privacy standards by which we can evaluate different privacy policies. They tell us what to look for when making our assessments about the benefits and harms of different privacy policies and practices. They give us reasons for preferring one privacy policy statement to another. They suggest ways of modifying policies to make them better. But we should be aware that when reading commitments expressed by an organization in their privacy policy, there may also be other easily overlooked potential vulnerabilities that undermine those commitments.

4.2.4 Conclusion

The core value framework of privacy, the balanced privacy framework, and the balanced privacy model provide us with a set of standards with which to assess policies even in situations where no previous policies exist and with which to assess other value frameworks when disagreements occur. If we respect others and their core values, i.e. take the ethical point of view, then privacy policies can be ranked at least roughly – some privacy policies can be judged to be better than others.

When a privacy policy has been changed, it is important that consumers are being notified and made aware of the organization's new privacy policy. Consumers who know in advance about businesses' practices regarding personal information could make an informed and voluntary choice as to whether or not to deal with that online company. By having an explicit note of privacy policy changes in which consumers were made aware of new practices and its effects, consumers could inquire specifically into how personal information about them is used in subsequent applications by those companies with whom they transact, and these consumers could then be able to make informed choices.

Though many organizations are taking strides to improve their privacy practices, and consumers are becoming more privacy-aware, it remains a tremendous burden for users to manage their privacy. As discussed earlier, the health organizations recommend that customers identify each site's sponsor; check the date of the information posted; verify that the material is factual information, not opinion; visit four to six sites; and read a site's privacy policy very carefully. For example, consider that organizations only have to define one privacy policy, but users are expected to read the policy of every Web site with which they interact. So it is no wonder that the minority of consumers follow the recommended protocol thoroughly.

The privacy policy should be consistently available, with the date of the latest revision clearly posted. This usually appears at the bottom of the page. However, the revision date does not sufficiently describe the type of change that occurred. If changes are unspecified, they are almost uncontrollable to the user. If the user has to read the whole privacy policy every time and compare between the new and old, it is not necessarily user-friendly.

An ideal privacy practice is both open and fair, and it would require the explicit consent of a customer to have his or her data used for new purposes. Following the balanced privacy framework, with its requirement of informed consent, data must also be provided in some way about how the acceptable

rules – e.g. the parameters and limitations of uses of the data about them – will be in practice. According to the balanced privacy model, it would seem to be the duty of the organization to inform customers about the change of privacy policy, and not the duty of customers to discover it for themselves by studying the matter during every visit to the web sites. All involved consumers need to be told explicitly that information about them is being used in new activities, since it would not be reasonable to expect the average consumer to be aware of new practices. If a company makes any changes to its privacy policy, the practice should let the customer know the effective date of the changes and provide a mechanism for the customer to understand what has changed. The mechanism should also consider not only the previous visit of the user but also notice the difference between a new and a previous situation showing changed fragments.

4.3 Visibility Category Scheme

This section proposes visibility and invisibility categories. The presented categorization scheme aids in evaluating privacy from the viewpoint of the consumer who wants their privacy protected and does not want to be misled by hidden tactics that can undermine consumer privacy.

The categorization scheme expresses four sub-categories that must be considered when evaluating an organization's privacy policy, specifying system requirements, and designing Internet software. The categorization scheme reflects the visible and hidden natures of privacy management practices, which are studied within the context of privacy protection and vulnerability. The categorization scheme is proposed to aid in the design of Web sites to focus on visibility and protection, but also visibility and vulnerability. These two views reflect practices of the balanced privacy model, whether protective or vulnerability, in that they are immediately visible to the consumer.

4.3.1 Visible and Invisible Category

So far we have discussed the fact that Internet privacy policies are critical due to the increase in information collection from several sources and the possibilities to gather and merge information in many ways. A privacy policy should directly reflect an organization's privacy rules and practices no matter

what methods are employed to gather and subsequently use the data. Whenever an Internet consumer visits a Web site, a large amount of consumer information may easily become available to the Web site. Every day customers go online to get information about a medical condition or symptom, fill a prescription, get an insurance quote, participate in a chat room, or fill out a health assessment. All of these activities involve the exchange of information with or without the consent of the individual, and with or without their knowledge. The majority of data exchange between a consumer and a Web site is visible to the user, but there are many methods through which a Web site can gather information without the consumer being aware.

Very few users who have minor knowledge of the Internet realize that their activities may be placed under surveillance, but information such as a user's email addresses as well as the system and network characteristics of a user's computer are easily recorded by many of the Web sites during one visit. According to the study, mouse clicks and keystrokes are frequently recorded by Internet health companies. That means information about which Web sites a user visits, how long he or she stays there, and where he or she goes afterward are recorded. Even when a customer orders a medicine from an online pharmacy, transactional information about the purchase is recorded, and information about that particular transaction can be (and frequently is) used for future business decisions.

Visible privacy practices are performed in such a way that an average Internet user is aware of data collection while accessing Web sites with a browser using default security and privacy settings. Invisible privacy practices are performed in a hidden manner that requires users to take a proactive role in learning about Web site privacy practices (e.g. reading the privacy policy, setting the browser's security and privacy settings, learning about cookies, etc.). The properties of these two categories are defined in Table 2. Visible and invisible privacy practices are essential trust factors for organizations that participate in online business due to the capability to easily collect data in both visible and invisible ways. Subsequently, consumers provide personal information in either a conscious or unconscious manner. Any organization embarking upon online transactions should therefore be prepared to address privacy matters in advance, clearly, and openly. A description of privacy management practices should be available to users without requiring extensive searching and reading processes.

The visibility and invisibility categories are grouped into two major categories, the protective and vulnerability categories, for the analyses reported below. Figure 8 introduces a 4-field matrix. The four fields are used

to classify privacy policy items as: visible/vulnerability, visible/protective, invisible/vulnerability, or invisible/protective. It is important to distinguish between visible and invisible because they both influence Internet consumers and Web site companies, but each may be differently interpreted. For example, visible items may be used as trust indicators of the Web site to the outside world. This issue is discussed in more detail in Section 4.4 when privacy seal programs are presented. Invisible items may unknowingly introduce additional vulnerability to the consumers, for example, Privacy Policy Statement #10. Thus, it should be an important focus for specifying and designing Web sites because consumers will value invisible practices being made visible to them in a privacy situation concerning trust and risk. This section advocates transforming invisible practices into visible ones as a design rule to ensure consumers are better informed and more readily able to manage their privacy.

The proposed visibility categorization scheme in Figure 8 is summarized by four fields: the publicity principle, negative and positive voluntary principle, security, and threat. These form the focal points for the following discussion.

The publicity principle coupled with the positive voluntary principle characterizes companies that clearly express how they are going to process consumer information. The vulnerability privacy practices of such organizations should also be openly stated without the consumer needing to take additional measures. The publicity principle coupled with the negative voluntary principles refers to organizations with Web sites that clearly express how they are going to protect consumer privacy. Both those visibility sub-categories are important to enable users to make informed decisions regarding the use of their personal information, which is one requirements of the balanced privacy model.

Threat refers to those companies that obscure (whether intentionally or unintentionally) practices that introduce vulnerabilities associated with the collection, transmission, or use of personal information. For example, a Web site (e.g. the Privacy Policy Statement #10) that requires consumers to read a Web site's entire privacy policy each time he/she visits the site is a candidate for considering possible 'visibility' requirements. Such visibility requirements would ensure that users receive visible cues, for example, by email or embedded in their browser, that reflect the site's privacy practices.

Security refers mostly to invisible technical means to protect customer privacy. IT practitioners and security officers need to focus on technical measures necessary to provide a secure IT environment that effectively protects consumer privacy while informing consumers to ensure sound decision-making.

4-field	Vulnerability	Protective
Visible	Publicity principle Positive voluntary principle	Publicity principle Negative voluntary principle
Invisible	Threat	Security

Figure 8: Visibility Categorization Scheme.

Software engineers can benefit from the categorization scheme, as it will guide them during the development process of their online systems. Assessing existing policies and requirements for their position within the categorization scheme aids requirements engineers as they seek ways in which to better inform Web site users about privacy practices and ways in which to minimize existing and potential information vulnerabilities. The balanced privacy model indicates the target direction of Web site development. In other words, the most desirable kind of Web site is one that emphasizes consumer trust and protection by implementing visible and protective items. The primary challenge is how to convert invisible and vulnerability items to visible and protective items. However, it is not possible to convert all vulnerability items to protective items. Therefore, at the very least it is important to convert invisible items to visible items to support Privacy-on-Demand and Service-on-Demand functions.

4.3.2 Coding Scheme

The coding scheme that was used to categorize the items extracted from these policies according to the visibility categorization scheme is presented next. During the categorization process, it was assumed the user's web browser maintains the default privacy/security settings.

Visible and protective items are categorized by analyzing each item and asking, "*Does this item support the core value framework of privacy and is it apparent to the user without reading the privacy policy statements?*" Consider the item I_{14}: `OPT to receive emails from our company`; this item clearly protects the user's privacy, because the user can decide whether or not to receive emails from the Web site enterprise and it is visible to the user without reading the privacy policy statement. This item is categorized as a visible and protective item, because the user is able to choose whether or not he/she chooses the positive or negative voluntary principle. In addition, this item supports the balanced privacy model.

Visible and vulnerability items are categorized by asking: "*Does this item conflict with the core value framework of privacy and is it apparent to the user without reading the privacy policy statement?"* Consider the item I_{15}: `USE member profile`. This item is categorized as a vulnerability item, because the user must give some personally identifiable information before he/she can continue further at the Web site, there is no other choice possibility. It does not support the balanced privacy model. But gathering information is an open process and the user consciously provides information; therefore, the item is categorized as a visible item.

Invisible and protective items are categorized by asking: "*Does this item support the core value framework of privacy but is it invisible to the user without reading the privacy policy statement?"* Consider the item I_{16}: `PREVENT disclosing personal identifiable information (PII) of children under 13.` This item is categorized as an invisible and protective item because it clearly protects user privacy but a user will not know this unless he or she proactively reads the privacy policy. Typically invisible privacy management does not support the balanced privacy model sufficiently. There is no possibility for the customer to opt out of any service or privacy functions.

Invisible and vulnerability items are categorized by asking: "*Does this item conflict with the core value framework of privacy and is it invisible without reading the privacy policy statement?"* Consider the item I_{17}: `SELL aggregate information`. This item clearly threatens user privacy and it is impossible for the user to be aware of this practice without reading the privacy policy statement first. Therefore, it is categorized as an invisible and vulnerability item.

The analysis of 39 privacy policies yielded 226 items, each of which was easily categorized according to each of the four sub-categories. There were 1102 total hits (or occurrences)[64] of the 226 items. For example, the visible/protective item I_{12}: `NOTIFY consumer of change to privacy policy` had 12 hits of that particular item within our 39 privacy policies. It appeared in one of the seven health insurance Web site privacy policies, four of the ten drugstore Web site privacy policies, none of the six pharmaceutical company Web site privacy policies, none of the six medical institute Web site privacy policies and seven of the ten general health Web site privacy policies. Similarly, the invisible and vulnerability item I_{17}: `SELL aggregate information` appeared in four of the privacy polices; therefore, it had 4 hits. No items that overlapped classes were encountered. Table 7 provides an overview of the visibility categorization scheme and shows the number of hits for items that map to these four sub-categories.

Table 7: Hits of Visibility Items.

Visibility Categories	**Major categories**	**Health Insur.**	**Drug store**	**Pharm Comp.**	**Med. Inst.**	**Gen. Health**	**TOTAL Hits**
Visible	Vulnerability	13	26	14	25	100	178 (16%)
	Protective	18	76	32	30	140	296 (27%)
Invisible	Vulnerability	22	77	23	47	143	312 (28%)
	Protective	35	73	21	29	158	316 (29%)
TOTAL	Visible	31	102	46	55	240	474 (43%)
	Invisible	57	150	44	76	301	628 (57%)
TOTAL		88	252	90	131	541	1102

The next section discusses each of the sub-category schemes within the context of the analysis of Internet health care privacy policies in more detail.

[64] In this dissertation the term “hits” is used.

4.3.3 Summary of Findings

4.3.3.1 Visible and Protective Sub-Category

Items that are easily observed and evaluated by the user are categorized as visible items. Visible process typically occurs when a user fills out a form, sends emails, or responds to a survey. All of these circumstances require the user to actively and consciously decide whether or not to provide the requested information. It is considered a conscious process when the user knows he/she is voluntarily disclosing information and is able to prevent the disclosure if so desired. As a the result of the case study, 474 hits of visible hits were observed (43 percent).

The visible and protective sub-category implies that a user gives knowing consent to an Internet company to do something with information concerning his/her protective way. The visible and protective sub-category should define the target of a Web site company regarding its practices of information management, because it represents an organization with open data practices that aim to protect the consumer. It should also be an important target for IT practitioners when designing and implementing Internet web solutions, because it essentially defines the Web site's trust factors and supports the balanced privacy model. The visible and protective sub-category got 296 hits, which is 27 percent of the total.

4.3.3.2 Visible and Vulnerability Sub-Category

Organizations need a lot of information about their consumers to offer rich service function. The visible and vulnerability sub-category reflects the direct openness of the Web site organization to the customer and can therefore increase the customer's trust.

According to the balanced privacy framework, if the organization shows how it is gathering, using, and sharing information about a consumer, it will provide the user with the knowledge necessary to foster an informed opinion regarding the organization's privacy policy. The responsibility of understanding that the Web site receives customer information is then subject to the customer's consideration, and this supports the balanced privacy model. Therefore, it is important to take note of the visible and vulnerability sub-

category, and this should be a target of an organization's Web site when it is not possible to convert items to the visible/protective sub-category.

This sub-category got 178 hits, which is 16 percent of the total. This was clearly a minor sub-category.

4.3.3.3 Invisible and Protective Sub-Category

Typical to the invisible category is that the actions of an Internet company are impossible or difficult for a user to observe and evaluate without reading the privacy policy in advance. For example, in situations where consumer information is not voluntarily provided by the consumer yet the information is collected and possibly used by the Web site organization. This typically occurs when a company uses cookies to gather information about a user, tracks users' usage patterns, or discloses user information to business partners without the user's consent. Invisible items saw a total of 628 hits (57 percent of the total). When we consider that invisible items are more common than visible items, this verifies that consumers are vulnerable to the privacy practices of the organization.

The invisible and protective sub-category indicates that an organization views security and privacy requirements as trivial. Typical to this sub-category is that the item supports technical security, which does not reflect directly on the user without reading the privacy policy first. Because this sub-category is a protective one, it is also a promising target of Web site organizations, although there is no flexibility as the balanced privacy model suggests. The main weakness of this sub-category is that a user is not assured of security without reading the privacy policy, and the Privacy-on-Demand function is not supported. The invisible and protective sub-category got 316 of the hits, which is over 29 percent of the total.

4.3.3.4 Invisible and Vulnerability Sub-Category

The invisible and vulnerability sub-category denotes a legitimate threat to user privacy. The threat is real because the majority of customers are not willing take the time to read Web site's entire privacy policy each time he/she visits the site. Similarly, not all Internet users are informed about privacy practices, personal data management, and browser configuration. This sub-category is illustrated by an example where a user begins a dialog with a Web site by

searching for information about a particular health problem or interest. The Web site is already able to collect data from the user without any visible notice to the user. According to the study, this kind of gathering process is very normal for this sub-category. The user does not know what, why, and/or when information is gathered and how it is used thereafter. It is important to observe that a user has not voluntarily disclosed any data for the purpose of storing it in a database on the Web site. The entire storing process is invisible to the user and it is, therefore, a subconscious process to the user. This goes against the balanced privacy framework and it conflicts strongly with the balanced privacy model.

According to the study, 27 of 39 Web sites collect technical-oriented data about users. For example (see Privacy Policy Statement #2), item I_2: COLLECT domain name had 11 hits in the 39 analyzed privacy policies, and many of those Web sites shared that kind of information with third parties without asking for user consent. So this kind of collecting and sharing process can happen without the user's knowledge if he/she does not carefully study the privacy policy in advance.

This sub-category got 312 hits, which is 28 percent of the total. The fact that the most vulnerable sub-category (invisible/vulnerability) got so many hits makes this study more important and justified.

4.3.4 Conclusion

The categorization scheme presented in this section addresses the visible and invisible categories. It is based upon four sub-categories of privacy items. Each of these sub-categories should be considered when specifying privacy requirements, which must comply with existing privacy (and perhaps even security) policies to ensure that consumer privacy values are adequately respected and reflected in the corresponding system implementations. The scheme provides a conceptual visibility categorization framework for responsible and efficacious privacy management while also providing some basic elements and viewpoints for Internet application design according to the balanced privacy model.

The contribution of the categorization scheme is primarily intended for software engineers, privacy managers, and consumer advocates. Information technology (IT) practitioners need to realize that the interplay between visible and invisible methods in protective and vulnerability settings plays a critical role in privacy management and privacy policy. It is important to distinguish

between the visible and invisible categories because they both influence Internet consumers and Web site companies, but each may be differently interpreted. For example, visible items may be used as trust indicators of the Web site to the outside world, and invisible items may unknowingly introduce additional vulnerability to the consumers. Consumers will value invisible practices being made visible to them.

The proposed categorization scheme is effective for examining how privacy policy statements and their respective system requirements may be made apparent to a consumer without the consumer first having to read the privacy policy statement. The categorization scheme is proposed to aid in the design of Web sites to focus on features of visibility and protective, but also visibility and vulnerability. These two sub-categories reflect practices, whether protective or vulnerability, which are immediately visible to the consumer and they, therefore, support the balanced privacy model. One idea of the categorization scheme is to encourage software engineers and privacy managers to transform invisible practices into visible ones using the interactivity possibilities of the Internet.[65]

4.4 Trust Factors

So far we have pointed out that organizational privacy policies and privacy practices reflect an organization's perceived trustworthiness to those with whom it conducts business. From the consumer viewpoint, the visibility categorization scheme provides a context for evaluating the level of trust communicated by the Web site to the consumer. This section discusses other communication practices for evoking customer trust towards organization that are found in health care Web sites.

4.4.1 Background

Size and reputation have been most frequently named as factors that evoke buyer trust towards seller organizations in traditional industrial buyer-seller relationships (Doney and Cannon, 1997). Additionally, companies with strong trademarks are very good examples of business institutions which reflect trust.

[65] Section 4.2 included examples of different communications practices of privacy matters, which can now be evaluated more accurately using the visibility category scheme.

We have more trust in the organization which is previous known at least by name. Quelch and Klein (1996) point out that an Internet consumer will favor sites that represent an organization with which the consumer is already familiar from traditional channels.

The literature suggests that a store's size assists consumers in forming their impressions regarding the store's trustworthiness. It seems that a consumer's trust is positively related to the Internet store's perceived size, but the effect of size on trust might be contingent on the merchandise type. "*The more uncertainty, ambiguity, or ongoing dependence on the merchant, ..., inherent in the type of service, the more importance the consumer might place on the store's resources, and hence the greater the influence of the perceived size of the organization in determining its trustworthiness*." (Jarvenpaa et al., 2000, p. 48).

Does perceived size affect consumer trust in an Internet health provider? Some health providers in the sample certainly seem to think so. At least health providers invest in web-page banners boasting of their size:

> *"Pharmacia Corporation is one of the world's fastest-growing pharmaceuticals companies with a strong portfolio of products, a robust pipeline of new drugs in development, and a commitment to improving health and wellness for people around the world "*
> (Pharmacia[66]).
>
> *"Pfizer Inc is a research-based pharmaceutical company with global operations"*
> (Pfizer[67]).
>
> *"Over 1,000,000 customers insured nationwide"* (eHealthInsurance.com®[68]).
>
> *"Over a million people have compared and saved 20% to 65% on their prescription purchases by finding the lowest online prices"* (DestinationRx[69]).

Lohse and Spiller (1998) speculate that the reputation of the physical store will influence the perceptions of an online site. It seems that a consumer's trust is positively related to the store's perceived reputation (Jarvenpaa, et al., 2000, p. 63).

---

66 May 18, 2002 at http://www.pnu.com
67 May 18, 2002 at http://www.pfizer.com/main.html
68 May 18, 2002 at http://www.ehealthinsurance.com
69 May 18, 2002 at www.destainationrx.com

Does perceived reputation affect consumer trust in an Internet health provider? Some Internet companies certainly seem to think so, although it seems not to be as common as expressions about the size of the company. Health providers have the opportunity to collect and publish testimonials regarding the quality, value, and efficiency of their service, and some health providers publish stories and customer testimonials on their sites attesting to their reputation.

> *"Your site is wonderful and informative. This will be our number one site for all our questions about medications" – Janice M.*[70]
>
> *"I used my card today for the first time. I couldn't believe that I saved 50% on my prescription medication" – Sandra H.*[71]

The ease of gathering opinions online from consumers who have used Internet services makes this practice particularly effective.

In the case of minor companies, prospective customers can be expected to be especially interested in a health provider's practices. Additionally, less well-known health providers might be able to build and promote their reputations by describing their principles and by quoting their policies. The welcome page of the studied online health providers, for example, proclaims in many different places that it honors customers' privacy. Other indicators of perceived trustworthiness are used, including respect for core values.

> *"Privacy is Central to the Doctor-Patient Relationship ... In medical school, and as a doctor, I learned first-hand the importance of protecting my patients' privacy. I carried that concern to Washington, and as Surgeon General I supported many privacy initiatives ..., I am accurately aware of the importance of maintaining the individual's privacy. The Internet is an ever-changing environment. But I want each person that comes to our site to know that we at drkoop.com not only respect your privacy, but actively work to protect it."*
>
> (C, Everett Koop, M.D., DrKoop[72]).
>
> *"PRESCRIPTIONONLINE.COM believes in a higher level of patient care than one would normally be afforded on the Internet. We believe our patients deserve a better caliber of*

---

70 "Customer's opinion", DestinationRX May 18, 2002 at http://www.destinationrx.com
71 "Customer's opinion", DestinationRX May 18, 2002 at http://www.destinationrx.com
72 May 18, 2002 at http://www.drkoop.com

> *personal care than they would receive at a traditional pharmacy."*
> (PRESTCRIPTIONONLINE.COM[73]).
>
> *"WellMed, continuing to lead the way in Privacy and Security – It is core to our business. Nothing is more important than people having access to their own health information in a way that is totally private and secure. So, together with Intel, we've created a credential and authorization system that allows individuals access to their health information from anywhere at any time, in a completely secure environment"*
> *(Craig Froude, President and CEO, WellMed[74]).*

Although such claims lack the definitiveness of a statement about technical means and policy practices, they presumably go some way towards increasing consumer estimates of perceived trust.

4.4.2 Privacy Seal Program

The effect of reputation on trust seems to be considerably stronger than the effect of perceived size on trust (Jarvenpaa et al., 2000, p. 63). If perceived reputation is an important factor in creating consumer trust, it might be particularly important for those health care companies who are not the largest in their field. This prompts interesting questions regarding sensitive issues between customers and companies. Health professionals are often apprehensive about the reliability of online health information and wonder how consumers can possibly find good Web sites in the untamed wilderness of the Internet (Fox and Rainie, 2002, p. 10). In an environment where any quack can create a credible-looking Web site and promote all manner of questionable "*cures*", how can Internet users know what Web site will most benefit them? What signals of quality should they seek? Without an indication of large perceived size, prospective customers can be expected to be especially interested in a health provider's reputation. How can a small Internet site evoke trust in the eyes of the consumer?

Web sites sponsored by stores that already enjoy an excellent consumer reputation have a head start in this regard and privacy seal goes even further. It seems natural that the specific innovations and particular institutional

---

[73] May 18, 2002 at: http://www.prescriptiononline.com
[74] May 18, 2002 at: http://www.wellmed.com

instruments of the Internet evolve as a result of the interplay of two fundamental needs. One is the economics of scale associated with the growing volume of the Internet, and the other is the privacy need of users. A mechanism that has the potential to realize both needs is a privacy seal program. Surely the causation of a privacy seal program ran in both ways (i.e. an organization and a customer), but when we look at the development of such a voluntary basis mechanism, we see that the evolution process has been a long one. It is not a new idea to use different kinds of seals; for example, protection of the bona fide purchaser was not originally a part of the common law. However, in commercial disputes the good faith principle was used earlier and on a much greater degree (the basis of Roman contract law by A.D. 200). It first evolved out of the fair bonds, which validated sales at fairs by affixing a seal to the bond. Originally this was a voluntary measure – the custom of fairs allowed debts to be contracted by witness. Eventually though, the desire to avoid fraud and at the same time increase revenue led to a law requiring that all sales be recognized by a sealed bond. Once sealed, the bond could only be invalidated by proving that seal had been forged (North, 1990, p. 129).

Some sites have responded to the public's concern regarding privacy and security on the Internet through self-regulation. To head off possible wider federal Internet privacy legislation, several professional organizations and trade associations have developed or are developing standards and seal programs to address privacy, security, and quality on the Internet. Standards and Seal programs that are in development or have been developed include:

- Association of American Health Plans, AAHP Principles for Consumer Information In an E-Health Environment, http://www.aahp.org;
- American Health Information Management Association, Recommendations to Ensure Privacy and Quality of Personal Health Information on the Internet, http://www.ahima.org/infocenter/guidelines/tenets.html;
- Health On the Net Foundation, HON Code of Conduct, http://www.hon.ch/HONcode/Conduct.html;
- Hi-Ethics, Ethical Principles for Offering Internet Health Services to Consumers, http://www.hiethics.org;
- International Society for Mental Health Online, Suggested Principles for the Online Provision of Mental Health Services, http://www.ismho.org/suggestions.html;

- Internet Healthcare Coalition, eHealth Ethics Initiative, eHealth Code of Ethics, http://www.ihealthcoalition.org/ethics.html;
- National Association of Boards for Certified Counselors, Standards for the Ethical Practice of WebCounseling, http://www.nbcc.org/ethics/webethics.htm;
- TRUSTe and Hi-Ethics, E-Health Seal Programs, http://www.truste.org/programs/pub_ehealth.html;
- URAC and Hi-Ethics, Health Web Site Accreditation, http://www.urac.org/programs/technologyhws.htm

A seal of approval for the quality of content of a Web site is important to consumers. URAC released a study in May 2001 showing that almost 80 percent of consumers said a quality seal on a health Web site was extremely important or very important to them, and over 70 percent of customers prefer that a private, nonprofit organization administer a health Web site accreditation program (URAC, 2001b). Although compliance with a privacy policy seal is voluntary and there are few, if any, enforcement mechanisms, a privacy seal program is more than an incentive issue against the opportunism possibility of a company in the Internet world of fundamental uncertainty, where capabilities, knowledge, and aims differ among actors.

In a sense, privacy seal organizations complicate privacy policy since the user does not attempt the challenging task of reading and understanding the policies themselves (Fox and Rainie, 2002; Earp and Baumer, 2003). The most significant facts about the privacy seal program are trust and ease. For example, the seal provided by TRUSTe appears to be quite comforting to users. However, many users are unfamiliar with what the privacy seal program truly means. A 2002 survey[75] in the U.S. revealed that the minority of Internet users indicated that they were familiar with privacy seal programs such as TRUSTe, BBBOnLine, and CPA WebTrust. The result is interesting because it could mean that there is hidden potentiality that should be applied more effectively. The following studies whether some of the most used privacy seal programs, TRUSTe[76] , BBBOnLine[77], and HONcode[78], have the potentiality to support the balanced privacy framework and the balanced privacy model.

TRUSTe is an independent, non-profit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair

[75] http://www.theprivacyplace.org
[76] http://www.truste.com/
[77] http://www.bbbonline.com/
[78] http://www.hon.ch/

information practices. The seal ensures that TRUSTe has reviewed the licensee's privacy policy and as required of TRUSTe licensees, the site must inform users of at least the following:

- What personally identifiable information about the users is collected;
- What organization is collecting the information;
- How the information is used;
- With whom the information may be shared;
- What choices are available regarding collection, use, and distribution of the information;
- What kind of security procedures are in place to protect the loss, misuse, or alteration of information under Internet service control; and
- How the users can correct any inaccuracies in the information.

If we consider the list very carefully, we can state that it is not particularly stringent and does not reflect a real commitment to user privacy; merely openness about what degree of user privacy is supported. TRUSTe requires licensees to disclose their privacy practices and adhere to established privacy principles based on the fair information practices. This is an admirable service and evidence exists that it has brought about the protection of user privacy in a very real way. The list reflects some commitment to the balanced privacy framework and the balanced privacy model. However, users should be alarmed by the privacy policies of some Internet services displaying this supposed "*commitment to user privacy*". As long as a privacy policy admits that user information is sold, leased, etc., the Internet service is eligible for a TRUSTe privacy seal. For example, some TRUSTe licensees in the sample sell or share their user email lists with other companies, allowing these third parties to send customers email solicitations.

The BBBOnLine privacy seal is posted on Internet services for which the merchant has met the Better Business Bureau's privacy program requirements regarding the notification, choice, access, and security of personally identifiable information collected online. These Internet services commit to abide by their posted privacy policies, and agree to comprehensive independent verification by BBBOnLine. These organizations must post privacy policies stating at least:

- What personal information is gathered;
- How it will be used;
- Choices the users have in terms of use; and
- The policy must verify security measures taken to protect gathered information.

The BBBOnLine privacy seal program is very similar to TRUSTe; users are partially given a false sense of high security when they encounter a BBBOnLine seal since they do not realize that an Internet service can display it regardless of whether or not a privacy policy truly protects user privacy. There are many differences among organizations of privacy seal programs, for example, Better Business Bureau is an organization that has been around for almost a century and it was a brand before the Internet. Therefore, it has the credentials that a relative newcomer such as TRUSTe lacks.

HON Code of Conducts (HONcode) differs from the preceding ones in that HONcode sets a universally recognized standard for responsible self-regulation. It defines a set of voluntary rules designed to help Internet service practice responsible self-regulation and to make sure the user always knows the source and the purpose of the information he or she is reading and disclosing. HONcode is today the most widely endorsed set of ethical guidelines for medical and health Internet services developers. It confirms that an organization respects and pledges to honor the 8 principles. Three of the most useful principles[79] concerning the study focus are briefly presented here.

- Confidentiality: Confidentiality of data relating to individual patients and visitors to a medical/health Internet service, including their identity, should be respected by the health provider. The health provider should undertake to honor or exceed the legal requirements of medical/health information privacy that apply in the country and state where the health service and mirror sites are located.
- Honesty in advertising and editorial policy: If advertising is a source of funding it should be clearly stated. A brief description of the advertising policy adopted by the health providers should be displayed on the site. Advertising and other promotional material should be presented to viewers in a manner and context that facilitates differentiation between it and the original material created by the institution operating the site.
- Authority: Any medical or health advice provided and hosted on this site should only be given by medically trained and qualified professionals.

Because privacy protection is a quality-dependent issue, it may be positive that the privacy seal programs are, especially the HONcode seal program, intended for self-regulation. Extrinsic rules may destroy the workers' intrinsic motivation, leading to a lessened level of quality-weighted effort (Kreps,

[79] The whole list is available at http://www.hon.ch

1997). Of course, intrinsic motivations are not always superior to extrinsic rules and incentives, but thiscould be an effective addition to high standard privacy management. Self-regulation can be very effective for managing the users' privacy protection, but one challenge is how the user can be guaranteed that in the Internet service context. This combination of intrinsic motives and extrinsic incentives might be one solution to achieve a high level of customers' privacy protection and good changes in terms of offering Internet health services extensively with trust. This is discussed in more detail in Section 4.7.

4.4.3 Seal Count Analysis

This section presents the main results of the analyses of 39 Internet privacy policies and the use of major category schemes to examine privacy seal programs in health care Web services.

The primary variables of interest for the analyses were the Internet service type (pharmaceutical companies, online drugstores, insurance companies, medical institutes/disease-specific sites, and general health information sites), the seal number, and the protective and vulnerability item hits. The analyzed Web sites, the protective category item hits, the vulnerability category item hits, and the seals are presented in Table 8.[80]

[80] A plus sign means that a Web site had the seal label on the Web site and a #-mark means that two extreme observations AFLAC and MedScape were dropped out of the following analyses.

Table 8: Analyzed Internet Web sites and Privacy Seals

Sites	Protection Goals	Vulnerable Goals	TRUSTe	BBBOnLine	HON	Others	Pharmaceutical	Health Insurance	Online Drugstore	Med.ical Institutes	General Health
Bayer	9	9					x				
Glaxo Wellcome	6	7					x				
Lilly (Eli)	2	5					x				
Novartis (Ciba)	20	5					x				
Pfizer	4	3					x				
Pharmacia Upjohn	12	8	+		+		x				
AETNA	6	5						x			
AFLAC#	1	1						x			
BCBS	15	7						x			
CIGNA	8	5						x			
eHealthInsurance	9	8	+	+				x			
Kaiser Permanente	5	1						x			
OnlineHealthPlan	8	9	+					x			
CornerDrugstore	17	9	+						x		
DestinationRX	17	18	+			+			x		
Drugstore	17	14	+			+			x		
Eckerd	9	6				+			x		
HealthAllies	13	6	+	+					x		
HealthCentral	15	12			+				x		
Ivillage	23	19							x		
PrescriptionOnline*	10	4	+			+			x		
PrescribtionByMail*	11	7	+						x		
WebRX*	18	7	+						x		
Nat. Inst. of Health	5	11								x	
Centers for Disease Control/Prevention	7	9								x	
Breast Cancer	4	5								x	
AIDS Treatments	5	5								x	
Am Cancer Society	24	22								x	
Am Diabetes Ass.	14	20								x	
Health Finder	9	10									x
Merck-Medco	40	21				+					x
WellMed Tools	13	21				+					x
MyHealth Tool	43	22				+					x
WellMed	33	23	+	+	+	+					x
WebMD Health	48	39	+		+	+					x
WebMd Practise	25	29	+		+	+					x
DrKoop	25	19									x
MedScape#	52	43									x
HealthScout	10	16			+						x
Total	612	490	13	3	6	10	6	7	10	6	10

Within the 39 Internet Web sites analyzed, the seal number ranged from zero to eight seal counts. In addition, although affiliation with a professional privacy trusted organization might increase the credibility of a health care company in the eyes of a prospective customer, only 19 of the Web sites in the sample posted this information.

The sensitive nature of health information and the assertions of "*commitment to user privacy*" indicate some of the differences that might be expected. The propositions of the study are presented in Table 9.

Table 9: Seal Count Propositions.

Propositions
Proposition 1: *The number of protective items in a health care privacy policy will depend on whether there is a seal or not on the Web site that posts that policy.*
Proposition 2: *The number of vulnerability items in a health care privacy policy will depend on whether there is a seal or not on the Web site that posts that policy.*
Proposition 3: *The number of protective items in a health care privacy policy will depend on whether there is one seal or more on the Web site that posts that policy.*
Proposition 4: *The number of vulnerability items in a health care privacy policy will depend on whether there is one seal or more on the Web site that post that policy.*
Proposition 5: *The proportion of protective items vs. vulnerability items is positively associated with the number of seals of that service.*
Proposition 6: *The number of seals on a health care Web site will depend on the service type of the site that posts that policy.*

These propositions were tested using analysis of variance (ANOVA) and t-test paired observations using the SPSS program (version 10.1). The rejection criterion for the overall test of significance in the ANOVA and t-test was set at 0.05.

First Proposition 1 and Proposition 2 are tested i.e. the study setting where health sites are divided into two groups. The first group is collected from those health sites that do not have any seal on their Web sites, and the second group is collected from the Web sites with at least one seal on their Web sites.

The means and standard deviations of protective and vulnerability item hits per two groups are summarized in Table 10.

Table 10: Means of Protective and Vulnerability Item hits per Two Seal Groups.

Report

Seal		Protective	Vulnerable	Total
No Seal	Mean	10,61	9,28	19,89
	N	18	18	18
	Std. Deviation	7,601	6,406	13,132
Seal (one or more)	Mean	19,37	14,68	34,05
	N	19	19	19
	Std. Deviation	12,437	9,298	20,638
Total	Mean	15,11	12,05	27,16
	N	37	37	37
	Std. Deviation	11,150	8,373	18,599

The division between the two groups is balanced (18 sites vs. 19 sites). Mean values in the case of the group Seal are much bigger than in the case of the group No Seal. This indicates that Proposition 1 and Proposition 2 will be supported.

In Figure 9, protective item hits are represented by quartiles per two groups.[81]

[81] Median: No Seal = 7.50 Seal = 15.00.

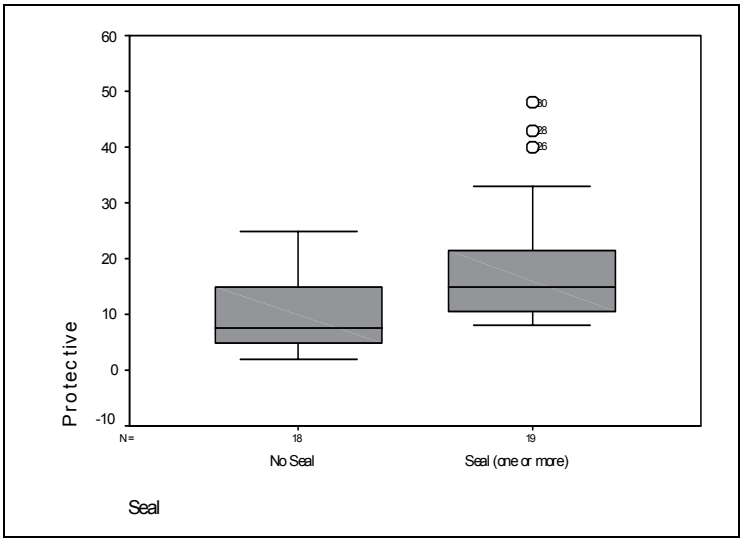

Figure 9: Quartiles and Median of Protective Item Hits per Seal Indicator.

The first proposition states that the number of protective items for a health care privacy policy would depend on whether there is a seal or not on the Web site that posts that policy. Highly significant differences (t-test, p=0.003) between the two groups were found, thus supporting Proposition 1. This finding is positive for the customers who hope that a health Web site with privacy seal program focuses more on expressing how they protect customer personal information than in the case of no seal. They seem to have commitment to user privacy.

In Figure 10, vulnerability item hits are represented by quartiles per two groups. [82]

[82] Median: No Seal = 7.00 Seal = 12.00.

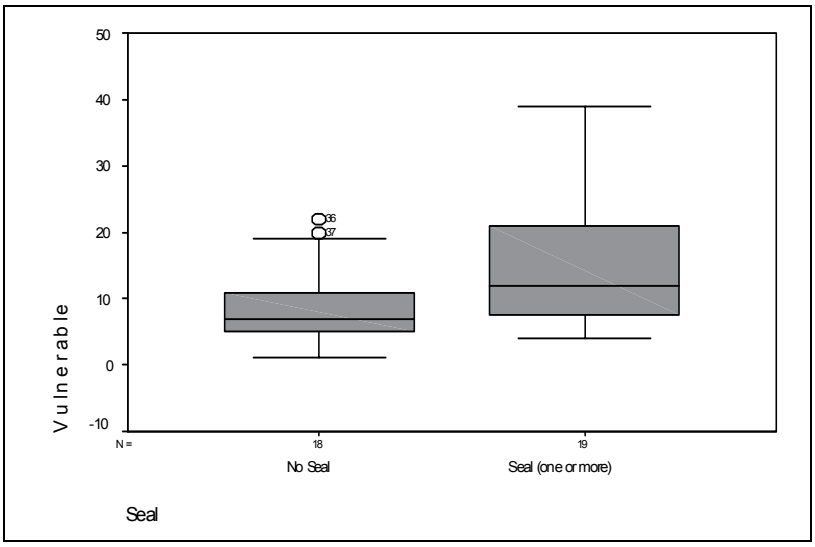

Figure 10: Quartiles and Median of Vulnerability Item Hits per Seal Indicator.

The second proposition states that the number of vulnerability items for a health care privacy policy would depend on whether there is a seal or not on the Web site that posts that policy. Significant differences (t-test, p=0,037) between the groups were found, thus supporting Proposition 2. This finding is even alarming for customers who hope that the privacy policy seal means a reduction in uncertainty and risk for the Internet customer. This finding also means the user, who does not want to be misled by hidden tactics, has to carefully read all privacy policy statements, even if there is a seal on the Web site.

Three groups are used for exploring Proposition 3 and Proposition 4. The first group includes a health Web site where the number of seals (i.e. no seal) is zero. The previous group Seal will be separated into two groups. One group is collected from health Web sites that have one seal, and the other group contains all those health Web sites that have at least two different seals on their Web sites. We test if there is any difference between Group 2 and Group 3, and if there is a positive association between the number of seals and the number of protective and vulnerability items.

The means and standard deviations of protective and vulnerability items per three groups are summarized in Table 11.

Table 11: Means and Deviations of the Major Category Items per Three Groups.

Report

seal count		Protective	Vulnerable	Total
0	Mean	10,61	9,28	19,89
	N	18	18	18
	Std. Deviation	7,601	6,406	13,132
1	Mean	18,40	13,00	31,40
	N	10	10	10
	Std. Deviation	12,633	6,429	17,595
2	Mean	20,44	16,56	37,00
	N	9	9	9
	Std. Deviation	12,885	11,854	24,321
Total	Mean	15,11	12,05	27,16
	N	37	37	37
	Std. Deviation	11,150	8,373	18,599

The division between the new groups is balanced (10 sites vs. 9 sites). Looking at Table 11, it seems as though could be a positive association between the number of seals and the mean of protective and vulnerability items, but because standard deviations vary so much it would be useful to analyze the propositions by variance analyses.

In Figure 11, protective item hits are represented by quartiles per three groups. [83]

[83] Median: Seal Count 0 = 7.50 Seal Count 1 = 14.00 Seal Count 2 = 17.00.

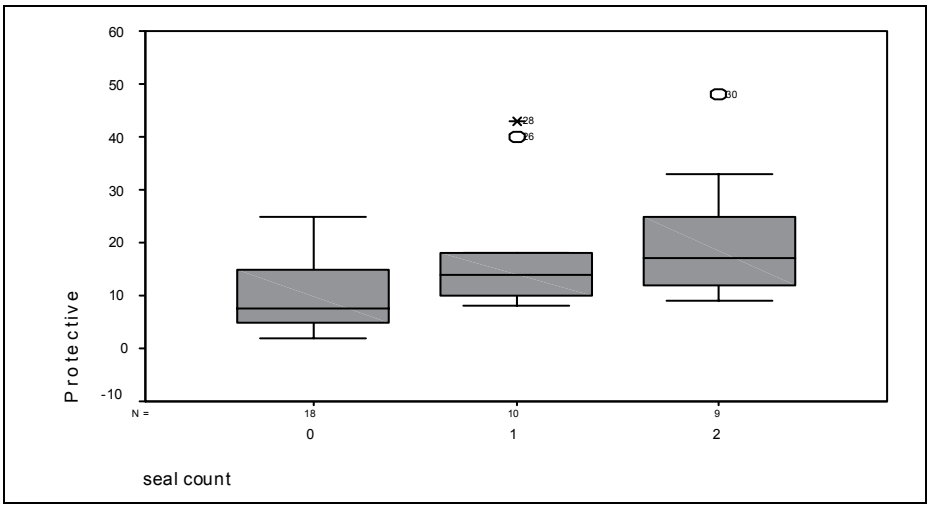

Figure 11: Quartiles and Median of Protective Item Hits per Three Groups.

The third proposition states that the number of protective items for a health care privacy policy would depend on whether there is one seal or more on the Web site. According to ANOVA (Tukey HSD[84] /Tamhane – analysis[85]), highly significant (p=0.016/p=0.011) differences among the three groups were found. According to multiple comparisons, there are no big differences in protective item hits between seal count 0 and seal count 1 (p=0.071/0.062), or between seal count 1 and seal count 2 (p=0.902/0.954). The only significant difference is between seal count 0 and seal count 2 (p=0.028/0.024). If we use p=0.05 as a rejection criterion, we can't conclude that there are more protective items found in a privacy policy if the seal count increases from 1 to 2, thus not providing support for Proposition 3.

This finding is negative for the users who hope that health Web sites with many privacy seal programs would focus even more on expressing how they protect user personal information.

In Figure 12, vulnerability item hits are represented by quartiles per three groups.[86]

84 SQRT – transform (for the demand of normality).
85 LN10 – transform (for the demand of normality).
86 Median: Seal Count 0 = 7.00 Seal Count 1 = 10.50 Seal Count 2 = 14.00.

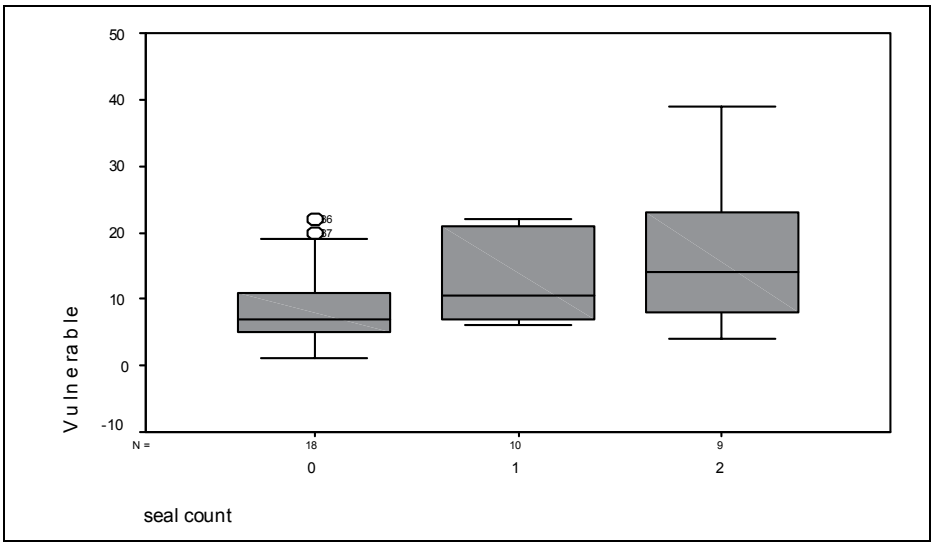

Figure 12: Quartiles and Median of Vulnerability Item Hits per Three Groups.

The fourth proposition states that the number of vulnerability items for a health care privacy policy would depend on whether there is one seal or more on the Web site. According to ANOVA (Tukey HSD/Tamhane – analysis[87]), significant differences were not found among the three groups. Based on that analysis, there are no significant differences of vulnerability items between seal counts (p=0.094/0.095), thus not providing support for Proposition 4. This result does not invalidate Proposition 2, because it stated that the number of vulnerability items for a health care privacy policy would depend on whether or not there is a seal on the health Web site that posts that policy.

Proposition 5 and Proposition 6 are tested next. Figure 6 provides the scatter image of protective and vulnerability item numbers per each health Web site. Based on the scatter image, it is difficult to say if the proportion of protective items in a health care privacy policy is greater than the proportion of vulnerability items for that policy. Therefore, in Figure 13 the result of function protective item hits minus vulnerability item hits per each health Web site is presented. [88]

[87] Same transforms as before for the demand of normality.
[88] Median = 3.000 Mean = 3.0541.

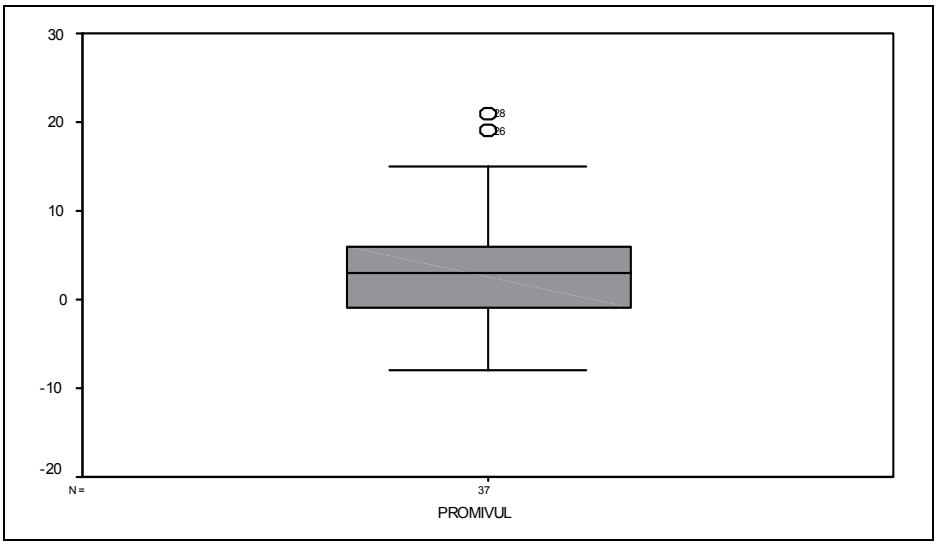

Figure 13: Quartiles and Median of the Function Protective minus Vulnerability Item Hits per Health Web sites.

Because the median (3.00) and mean (3.05) are much bigger than zero, it is supposed that the proportion of protective items in a health care privacy policy is greater than the proportion of vulnerability items for that policy. As expected, a high value (t-test, p=0.007) was found, which states that values differ significantly from zero.

The preceding argument probed the privacy situation as a whole, but next the same issue will be tested using the number of seals. It is important to note that the following sections will focus on the proportion of protective item hits per vulnerability item hits, thus the neutral value is 1.000 instead of 0.000.

In Figure 14, the proportions are represented by quartiles per three groups.[89]

[89] Median: Seal Count 0 = 1.045 Seal Count 1 = 1.536 Seal Count 2 = 1.231.

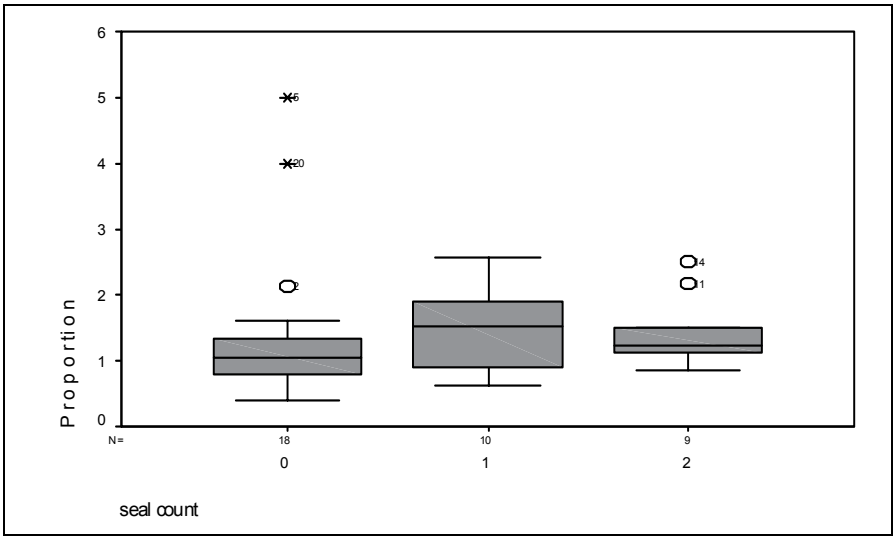

Figure 14: Quartiles and Median of Proportion Protective / Vulnerability Item Hits per Three Groups.

The fifth proposition stated that the proportion of protective items vs. vulnerability items would be positively associated with the number of seals of that site. Based on Figure 14, it seems very likely that the fifth proposition is not supported. All medians are greater than 1.000, but there seems to be no positive association with the number of seals. According to ANOVA, there are no significant (p=0.666) differences among the three groups, thus not providing support for Proposition 5. In the case of two groups (Seal/No Seal), there are no significant (p=0.365) differences between the groups either.

This finding is negative for the users who hope that a health Web sites with many privacy seal programs would focus more on expressing how they protect user personal information. The result indicates that the privacy seal programs do not mean the reduction of uncertainty and risk for the Internet user. But the findings that there are more protective item hits than vulnerability item hits gives a minor reason to consider high customer privacy. This is explored more closely in Section 4.5.

In Figure 15, seal counts are represented by quartiles per health provider's type.

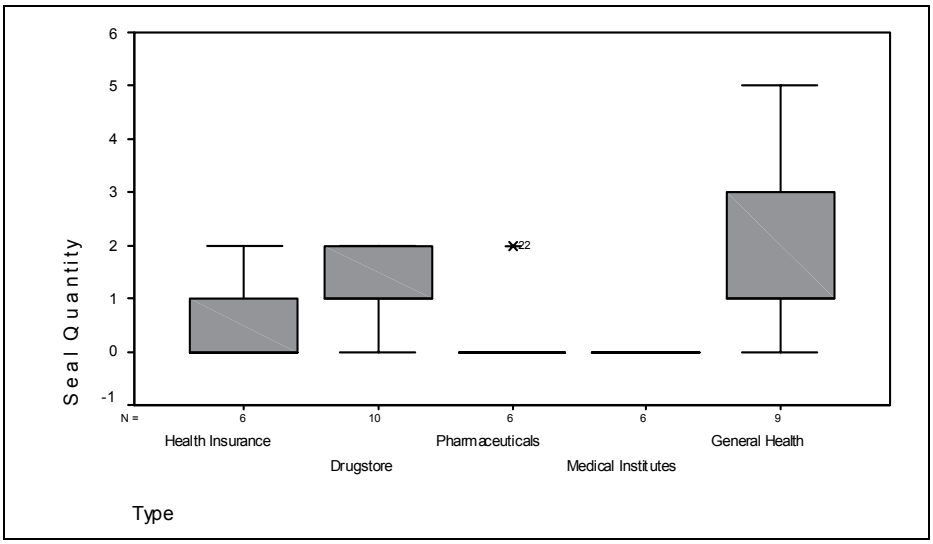

Figure 15: Quartiles and Median of Number of Seals per Health Provider's Type.

The sixth proposition states that the number of seals on a health Web site would depend on the health provider type. Significant differences between health provider types have been discovered, for example, none of the group of medical institutes had any seal on their Web site, and only one of the pharmaceutical companies had a seal (Pharmacia Upjohn). The other extreme is found in the group of online drugstore services, where nine in ten had at least one seal on their Web site. Considering Figure 15, it is supposed that the result (without any more analyses) is enough to make a positive conclusion and thus provide strong support for Proposition 6. This finding might reflect the fact that consumers tend to have less apprehension regarding the information practices in a non-retail industry (Earp and Baumer, 2003) and therefore there is no need to use privacy seal programs on the Web site of the medical institutes. Pharmaceuticals companies with strong trademarks are business institutions that reflect trust, and that might be the reason why they don't use any privacy seal programs on their Web sites.

4.4.4 Conclusion

In the health context, the perceived risk negatively influences willingness to use health services. Participating in a privacy seal program that already enjoys an excellent consumer reputation allows organizations to distinguish themselves from the thousands of online services in a way that is easily recognizable by online users and that will instill trust and confidence in their health service. One of the consequences of a privacy seal is that it reduces the consumer's perception of risk associated with opportunistic behavior by a health provider. "*For the most part the need for privacy is like good art, you know it when you see it. But sometimes our intuitions can be misleading"* (Moor, 1997, p. 28). We make constant use of metaphors, symbols, and rules whose meaning we do not necessarily understand thoroughly. The privacy seal programs are just some of those possible formats that are used even though we are still very far from having learned to make the best use of them.

The study indicates that the number of protective and vulnerability items in a health care privacy policy will depend on whether there is a privacy program seal or not on the Web site that posts that policy. But the user lacks the ability to make an actuarial determination of the likelihood of privacy invasion without the user first having to read the privacy policy statements. Although the most significant facts about the privacy seal program are trust, ease, and visibility, the study results indicate that the privacy policy seal does not mean the reduction of uncertainty and risk for the health Web site user without the user first having to read the privacy policy statement. Privacy seal programs might have the potential to provide that assurance, but they do not necessarily mean full privacy protection and security.

4.5 Variation of Privacy Practices

This section discusses the varieties of privacy policy content among 39 health care Web sites. The study focus is important for consumers who hope that they can "*predict*" privacy practices of the Internet service in advance without to take a very proactive role in learning about Web site privacy practices.

The current study (Anton, Earp, Bolchini, He, Jensen and Stufflebeam, 2003) points out that there is the lack of clarity in 40 online privacy policies from nine financial institutions that are covered by the Gramm-Leach-Bliley

Act (GLBA), which states that policies should be "*clear and conspicuous*[90]". They have used The Flesh Reading Ease Score metric[91] to test if it is reasonable to expect the target audience to understand the privacy policies. Their findings show that compliance with the GLBA "*clear and conspicuous*" requirement by the analyzed financial privacy policies is at best questionable. They found that most of the content was written at a high school or college reading level – much higher than the sixth-grade reading level recommended by experts concerned about consumers' ability to understand the information. "*A full understanding of what two thirds of these organizations are doing is perhaps only available to one sixth of the adult U.S. Internet population*." (Anton et al., 2003, p. 10).

If we compare the number of vulnerability and protective item hits and the proportion of protective item hits versus vulnerability item hits between different Web site types, we can test if privacy policy content differs significantly from Web site to Web site. If there significant variations are found, possible differences require users to take a very proactive role in learning about Web site privacy practices (e.g. reading the privacy policy and calibrating their understanding of different Web site policies), thus imposing a tremendous (and unfair) burden on the end user.

4.5.1 Content Variance Analysis

The primary variables of interest for the focused analyses were the kind of Web site (pharmaceutical companies, online drugstores, insurance companies, medical institutes/disease-specific Web sites, and Web sites of general health information) and the item hits of major categories. Prior to the data analysis, three tentative propositions are set forth. The assertions point toward some of the differences that might be expected. The presented theoretical backgrounds, for example, the analyses of legal issues and the analyses of privacy seal programs should be reflected in the following ways in the privacy policy contents. The propositions are presented in Table 12.

---

[90] Where clear and conspicuous notice is defined as "a notice that is reasonably understandable and designed to call attention to the nature and significance of the information in the notice".

[91] It is a metric for evaluating more complex texts and is often used both to evaluate school texts as well as legal documents (Flesch, 1949).

Table 12: Major Category Item Propositions.

Propositions
Proposition 7: *The number of protective items in a health care privacy policy will depend on the type of Web site that posts that policy.*
Proposition 8: *The number of vulnerability items in a health care privacy policy will depend on the type of Web site that posts that policy.*
Proposition 9: *The proportion of protective items vs. vulnerability items will depend on the type of Web site that posts that policy.*

If it is possible to make conclusion that Proposition 7 or/and Proposition 8 or/and Proposition 9 is/are supported, it means that the contents of privacy policies vary significantly between the studied health care Web sites. In that case, it is not surprising that customers may find it difficult to be aware of prevailing privacy practices expressed by health providers in their ("*unclear*" and "*inconspicuous*") privacy policies.

These propositions were tested using analysis of variance (ANOVA) and t-test paired observations using the SPSS program (version 10.1). The rejection criterion for the overall test of significance in the ANOVA and t-test was set at 0.05.

Table 13 illustrates the result of the study. It includes means and standard deviations of protective and vulnerability item hits per Web site type.

Table 13: Means of the Majority Category Items per Web Site Type.

Report

Tyyppi		Protective	Vulnerable	Total
Health Insurance	Mean	8,50	5,83	14,33
	N	6	6	6
	Std. Deviation	3,507	2,858	5,574
Drugstore	Mean	15,00	10,20	25,20
	N	10	10	10
	Std. Deviation	4,295	5,287	9,041
Pharmaceutical Companies	Mean	8,83	6,17	15,00
	N	6	6	6
	Std. Deviation	6,524	2,229	7,294
Medical Institutes/ Disease Spesific Sites	Mean	9,83	12,00	21,83
	N	6	6	6
	Std. Deviation	7,834	7,376	14,865
General Health Information	Mean	27,33	22,22	49,56
	N	9	9	9
	Std. Deviation	14,654	8,136	21,196
Total	Mean	15,11	12,05	27,16
	N	37	37	37
	Std. Deviation	11,150	8,373	18,599

The only case where the mean of vulnerability item hits is bigger than the mean of protective item hits is the case of medical institutes. The standard deviation of protective items in every case (except Drugstore) is bigger than the standard deviation of vulnerability items. The most significant value of standard deviation is found on the protective items hits of General Health Information.

In Figure 16, protective items are represented by quartiles per Web site type.[92]

[92] Median: Health Insurance = 8.00 Drugstore = 16.00 Pharmaceuticals = 7.50 Medical Institutes = 6.00 General Health = 25.00.

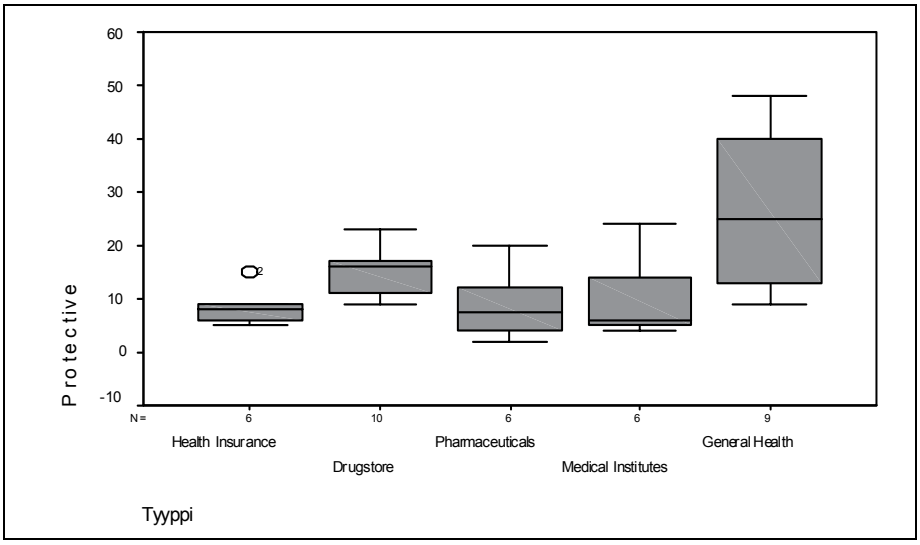

Figure 16: Quartiles and Median of Protective Item Hits per Web Site Type.

The seventh proposition states that the number of protective items for a health care privacy policy will depend on the type of Web site that posts that policy. Highly significant differences (p=0,001) were found among the five types of health care Web sites. This means that the number of protective items in a privacy policy will depend on the type of Web site, thus supporting Proposition 7.

When exploring this relationship in more detail, it can be observed that the Web sites of general health information generally require more protective statements in their privacy policies when compared to the Web sites of health insurance. According to multiple comparisons of ANOVA (Tamhane – analysis), the most significant difference exists between the group Health Insurance and the group General Health Web sites (p=0.022). Some differences between groups are not significant, for example, the ANOVA result between Pharmaceuticals, Medical Institutes and Health Insurance seems to be almost equal (p=1.000). The group Drugstore shows no significant difference if the rejection criterion of multiple comparisons is set at 0.05 between health insurance (p=0.070) or pharmaceuticals (p=0.515), although the median (16.00) of Drugstore is much bigger than Health Insurance (8.00) or Pharmaceuticals (7.70). The other nearly significant difference is between Pharmaceuticals and General Health (p=0.052), which is just a little bit greater than the rejection criterion.

In Figure 17, vulnerability item hits are represented by quartiles per Web site type.[93]

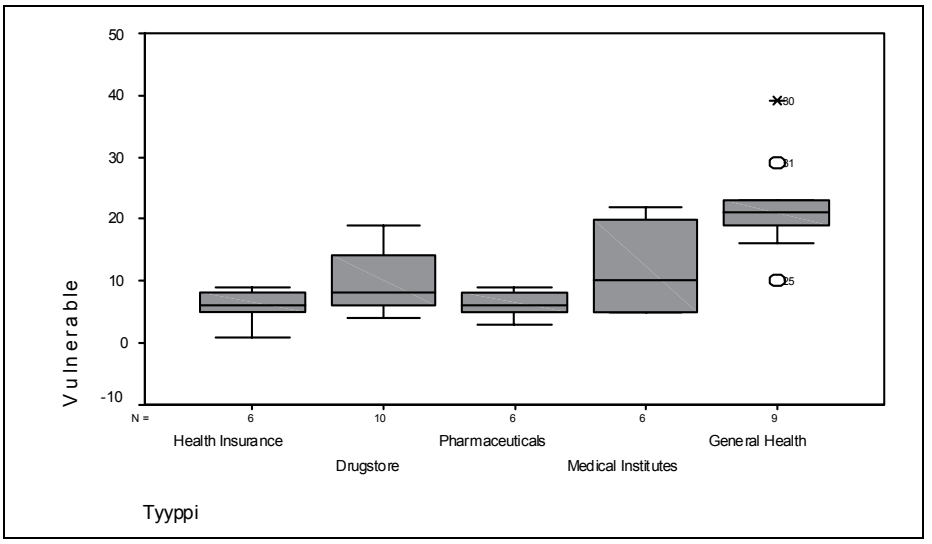

Figure 17: Quartiles and Median of Vulnerability Item Hits per Web Site Type.

The eighth proposition states that the number of vulnerability items for a health care privacy policy will depend on the type of Web site that posts that policy. Highly significant differences (p=0,000) were found among the five types of health care Web sites. This means that the number of vulnerability items in a privacy policy will depend on the type of Web site, thus supporting Proposition 8.

According to multiple comparisons of ANOVA (Tukey HSD – analysis), there are significant differences concerning vulnerability item hits between the group General Health and the other groups: Health Insurance (p=0.000), Drugstore (p=0.002), Pharmaceuticals (p=0.000) and Medical Institutes (p=0.032). Members of the group General Health Information often require more vulnerability items in their privacy policies when compared to the other four groups. The other differences are not significant. The group Drugstore

[93] Median: Health Insurance = 6.00 Drugstore = 8.00 Pharmaceuticals = 6.00 Medical Institutes = 10.00 General Health = 21.00.

has no significant difference in comparison with Health Insurance (p=0.364) or Pharmaceuticals (p=0.533). The median (8.00) of the group Drugstore is not much bigger than either Health Insurance (6.00) or Pharmaceuticals (6.00). Comparison between Health Insurance and Pharmaceuticals shows that the groups are almost equal (p=0.999).

When comparing total number (protective plus vulnerability items), the Proposition "*the number of items in a health care privacy policy will depend on the type of Web site that posts that policy*" is also supported (p=0.000) among the five groups. The most significant difference is between Health Insurance and General Health (p=0.009).

In Figure 18, the proportion of protective items per vulnerability item hits are represented by quartiles per five groups. [94]

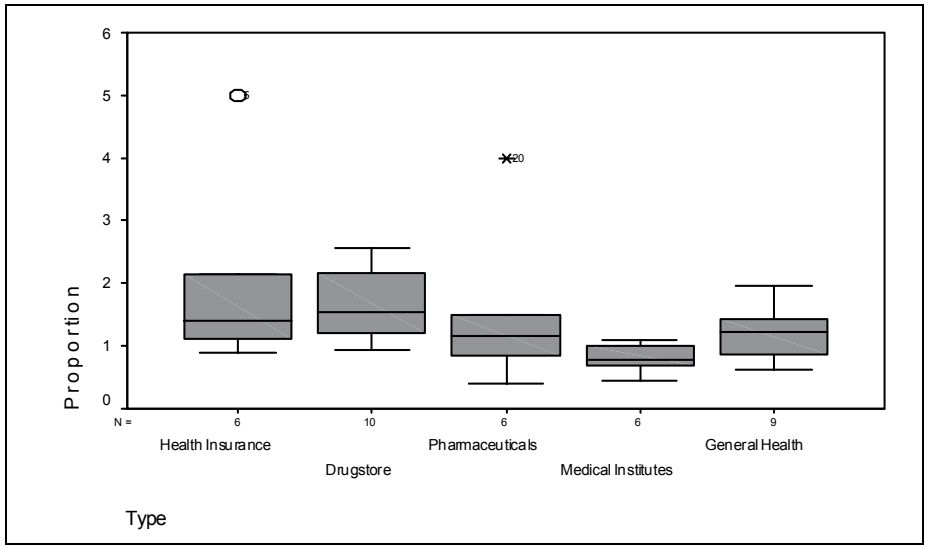

Figure 18: Quartiles and Median of Proportions Protective / Vulnerability Item Hits per Web Site Types.

The ninth proposition states that the proportion of protective items versus vulnerability items will depend on the type of Web site that posts that policy.

[94] Median: Health Insurance=1.400 Drugstore=1.536 Pharmaceuticals=1.167 Medical Institutes=0.789 General Health = 1.231.

According to ANOVA, there are no significant (p=0.093) differences among the five groups, thus not supporting Proposition 9.

One median was lower than 1.000 (Medical Institutes), which indicates that there are more vulnerability items than protective items found in those privacy policies but it wasn't significant difference according to the t-test (p=0.163). The analysis revealed one significant (t-test, P=0.001) observation, which states that the number of protective items for the group Drugstore is significantly larger than the number of vulnerability items for each individual Web site[95].

4.5.2 Discussion

The Web sites of the group General Health require more protective and vulnerability privacy statements in their privacy policies – the most significant difference is between the Web sites of Health Insurance and General Health. Web sites that support electronic commerce transactions widely, i.e. the transactional and interactive stages in the Internet maturity model stages (Stage 3 and Stage 4 in Figure 2) require many types of informationally-enriched processes and activities. It seems natural that Web sites require more policy statements.

Many General Health Web sites support health care tools and a lot of information about customers is received in those Web sites much information about customers. Many of them allow consumers to access and modify their personal information online, thus supporting the balanced privacy model. The subject matter items one expects to see in these Web site's policies include a lot of personally identifiable medical information, information transfer and storage and many others. In contrast, Web sites whose primary mission is information dissemination with few transactions (Stage 1 and Stage 2 in Figure 2, i.e. marketing and publishing) have little or no need to address the use of credit card information and many other similar pieces of information. Health Insurance and Pharmaceutical Web sites tend to require the least number of items. One reason could be that they are more normatively regulated and thus have less flexibility regarding how they manage personal information, and secondly their Web sites' primary mission seems to be information dissemination with few transactions.

[95] T-test result: 95% confidence interval of the difference ranges from 2.42 (lower) to 7.18 (upper).

The Web sites of Medical Institutions tend to require many vulnerability items but not so many protective items. One reason could be that consumers tend to have less apprehension regarding the information practices in a non-retail industry (Earp and Baumer, 2003). Additionally, it seems that some of the Medical Institutions' Web sites use law statutes in their privacy policies, and therefore there is no need to use many protective statements. Law statutes found in the study mainly include privacy protective issues. Consider Privacy Policy Statement #15 from the Centers for Disease Control and Prevention (CDC) and Privacy Policy Statement #16 from the American Diabetes Association Web site.

Privacy Policy Statement #15

> *"This site is maintained by the U.S. Government and is protected by various provisions of Title 18. U.S. Code. Violations of Title 18 are subject to criminal prosecution in Federal court."*

Privacy Policy Statement #16

> *"Protecting the privacy of the very young is especially important. For that reason, we adhere to the 1998 Children's Online Privacy Protection Act (COPPA) For more information visit the Federal Trade Commission's COPPA site at http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/adults.htm "*

The use of different statutes is an easy way to provide assurance of customers and could be an effective tool "*to call attention to the nature and significance of the information*". But there is a problem – the population's average literacy level concerning law issues. If there are problems in understanding privacy policies, and in the case of the law statutes the problem is supposed to be even more significant, then it is not reasonable to expect the target audience to understand the policy fully as discussed in Section 2.3. Moreover, low online health literacy limits many Americans' ability to understand what is available online (Baur, 2004). So it is not a surprise that those with more education and more Internet experience are more likely to search for medical advice online (Fox and Rainie, 2002). An educated consumer stands a better chance of getting better treatment, and the Internet can be a significant resource for that health education process. Online health information is not just a convenience – a report published in the New England

Journal of Medicine in June, 2003 found that Americans receive about half of recommended medical care. (McGlynn, Asch, Adams, Keesey, Hicks, DeCristofaro and Kerr, 2003).

4.5.3 Conclusion

This section has evaluated privacy policies with the intent to increase understanding of privacy policy literacy problems. It is an important matter because many privacy policies contain technical and confusing language (i.e. not natural language) that makes it difficult for the users to fully understand what they are agreeing to. If we compare the number of vulnerability and protective items between different Web sites, we can conclude that in spite of the many guidelines and criteria for the content and layout of these policies, privacy policy content inevitably varies from Web site to Web site. When formulating privacy policy, the raison d'etre of the company lies in its ability to provide coordination when divergent incentives exist between different stakeholders. We must look at privacy policies as such media for communicating and collaborating on information if we want to understand their real function; a function that, of course, it fulfils less perfectly as the message grows less comprehensible.

Web sites that support enriched information flow between third parties where a lot of information about customers is received and shared need a wide privacy policy of many vulnerability items, but they also need protective items. In contrast, Web sites whose primary mission is information dissemination with few transactions have little or no need to address so many privacy issues. Considering the balanced privacy model it seems that we will fail if we pursue one permanent privacy policy content. According to the balanced privacy model, flexibility and interactivity are important issues to consider widely. It seems natural that Web sites that support rich service functions require more policy statements for the reasons of the Privacy-on-Demand and the Service-on-Demand functions.

4.6 Modularity Category Scheme

This section presents a privacy framework that expresses the five organizational categories that must be considered when formulating and/or evaluating an organization's privacy policy and privacy management. These

categories reflect contractual commitments between organizations, social relationships between users and the organization, motivations of business, technology capabilities, and the whole of these encompassed within health care and Internet legislations.

4.6.1 Background

Some proposals and suggestions for how to deal with privacy issues involving information technology fall into one of two types of approaches: proposals that are technology-based and those that are legislation-based.

Since the inception of commercial activity on the Web, security has been perceived by some to be a significant barrier to the emergence of a consumer mass market on the Internet. Several researchers have provided various approaches to creating sufficient data protection for consumers. On the technological level, a lot of emphasis is put data protection and confidentiality issues to prevent unauthorized use.

Business and industry representatives in the electronic commerce sector suggest that virtually all privacy issues, including those generated by data mining, can be resolved through certain technical solutions. For example, there are many possibilities to use statistical data mining. Novel randomization tricks let enterprises compile statistics without putting individual records at risk (Pearson, 2003). Others point out that various privacy-enhancing technologies enable users to be anonymous in certain online commercial activities and transactions (Tavani 1999b, p. 271; Uslaner, 2000, p. 19). But there is no single answer to how privacy-enhancing technology can manage privacy issues widely, because technology will enable health providers and customers to be more responsive, productive, innovative, and resilient. Certain technologies pose new privacy concerns, depending on how they are used (Pearson, 2003).

The second type of approach, which is legislation-based, generally calls for increased normative protection such as extending current data protection laws and guidelines. For example, the differentiating and specializing features of data mining introduce privacy concerns that are not explicitly addressed in the existing privacy laws and privacy guidelines (Tavani, 1999b). Advocates of this position typically include privacy interest groups who lobby for stronger enforcement of existing privacy laws and guidelines, and they suggest that the legal protection of the right to online privacy within the U.S. should be strengthened (Michelfelder, 2001, p. 130). One advantage of legislation-based

proposals over those that are technology-based, such as proposals involving the use of privacy-enhancing technologies, is that legislation-based proposals are not limited in their application to privacy concerns involving technical artifacts. They are able to cover a much wider area of privacy issues, including those health processes and practices which are not computer-supported. On the other hand, legislation-based proposals do not appear to provide customers who might wish to opt-in to special features with a mechanism to do so according to the balanced privacy model. Certain customers might wish to opt-in to services that pose a minor threat to their privacy protection. Legislation-based proposals easily downplay the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings.

It would seem that neither of the two approaches considered so far in this section provides a fully adequate solution to the privacy issues from the perspective of the balanced privacy model. Michelfelder (2001, p. 129) gives us a third approach to consider: "*solutions to the problem of protecting informational privacy in cyberspace tend to fall into one of three categories: technical solutions, self-regulatory solutions, and legislative solutions*." Self-regulatory solutions rely on personally assumed responsibility, whether by an individual or a corporation, to determine and implement standards for protecting informational privacy. "*There are various ways in which these approaches can be combined: for instance, an individual, motivated to accept primary responsibility for protecting his online privacy, may turn to privacy-enhancing technologies to achieve that purpose, it still makes sense in discussing this topic to identify these three separate perspectives.*" (Michelfelder, 2001, p. 129). Some advocates of this view believe that the technological solutions can work hand-in-hand with certain voluntary controls and guidelines, and that there is no need for governments to enact stricter privacy legislation to respond to challenges posed by information technology (Michelfelder, 2001, p. 130). However, in order to protect their privacy, a relatively small number of savvy customers are devising their own "*opt-in*" policies and deciding that some Web sites are not worthy of getting their personal information. One in four Internet users has provided a fake name or personal information in order to avoid giving the Web site real information. But most users do not use the available privacy protection tools, perhaps because they are unaware of how Web sites work and how existing technologies can be deployed to protect them (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 3).

It is apparent that a more structured framework is needed to adequately consider privacy issues within a broader and more sensitive organizational context. So while privacy-enhancing technologies and legislation-based proposals provide a basic "*solution*" to privacy issues involving the use of personal information on the Internet, they both have weaknesses which need to be covered. Self-regulatory solutions and practices as widely understood might provide the support needed for that.

We will get a glimpse of what to consider when we think about Gotlieb's determination of (1995, p. 156) the core terms as follows: Privacy is a social, cultural, and legal concept, all three aspects of which vary from country to country. Confidentiality is a managerial responsibility: it concerns the problems of how to manage data by rules that are satisfactory to both the managers of data banks and the persons whom the data concerns. Security is a technical issue. It focuses on how the rules of data access established by management can be enforced through the use of passwords, cryptography, and similar techniques. In terms of protecting informational privacy on the Internet, all those aspects are needed to provide assistance when developing privacy policies for electronic commerce Web sites.

4.6.2 Five Modules

If privacy is understood as Gotlieb has described it, privacy management must be evaluated from several perspectives within an organization; these perspectives primarily include legal constraints, technical measures, business rules, social norms, and contractual norms. The modularity framework presented in this section addresses these five perspectives and aims to provide a conceptual framework for responsible and efficacious privacy management.

Information technology practitioners need to be aware of the interplay between those perspectives and realize that each plays a critical role in privacy management and privacy policy. The five categories and their relationships are illustrated in Figure 19. The legal category, in a sense, constrains the business rules, technical measures, social norms, and contractual norms of an organization. The technical category includes tools to support business objectives as well as social and contractual expectations; however, the limitations of technical measures, in turn, may constrain these objectives and expectations. The business category is contained within the legal category because legislation provides the minimum requirement for business practices. Technical items must pass through the legal and business filters. The business

category thus forms the foundation of the modularity framework, as business items are motivated by social and contractual norms and expectations between organizations and users. The focus of the social category is on relationships with consumers, while the focus of the contractual perspective is on contractual relationships with other partnering organizations (e.g. third parties).

The inner boxes, which are labeled as users, organization, and third parties represent the stakeholders that are influenced and/or constrained by the modularity categories. The relationship between an organization's Web site users and the organization is characterized as social in nature. Organizations and their users (or customers) interact in a cooperative way, exchanging goods, services, and or information. In contrast, the relationship between the organization and its third parties is characterized as contractual. The social and contractual relationships that exist between an organization and the constituent stakeholders are influenced, in turn, by business objectives, technical constraints, and possibilities and most actively by the legal obligation to adhere to the relevant legislation.

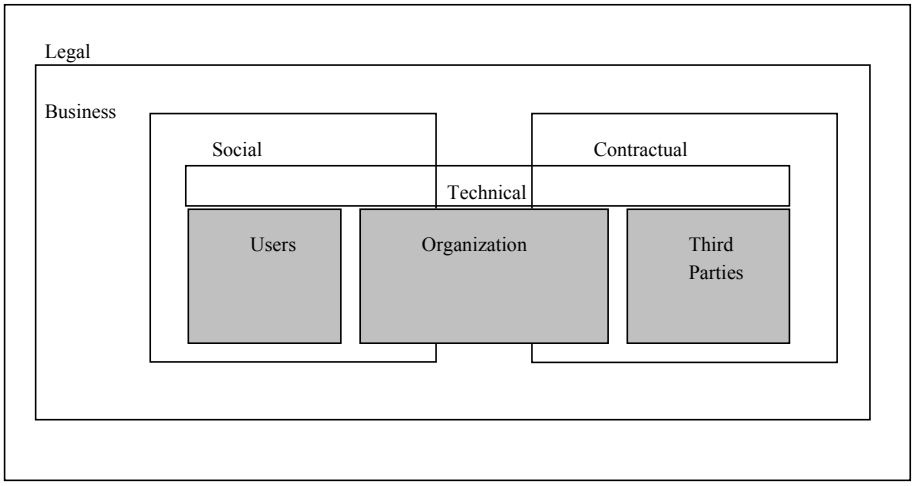

Figure 19: Modularity Categories for Privacy Management Framework.

All modularity categories play a key role in electronic commerce, especially when one considers that one weak link in the series of categories can make online organizations vulnerable to legal challenges, dissatisfied customers,

and/or strained relationships with other organizations. Consider an organization, for example, that sells their customers' personally identifiable information to third parties for profit. If this is not accurately expressed in the organization's privacy policy, then legal challenges become a potential threat to the organization. Similarly, consider a Web site that sends monthly email announcements to their customers but also provides customers with the option to "*opt-out*" of the email correspondence. When customers "*opt-out*" of such communication, but continue to receive such email correspondence anyway, then the organization may face dissatisfied customers.

4.6.3 Coding Scheme

To date the modular framework has been validated via its application in the analysis of 39 health care Web site privacy policies. The modularity categories were used to classify items that were extracted from the 39 privacy policies. Next, the coding schemes are presented. The categorization of the health care privacy policy items involves differentiating items according to the modularity categories of the framework.

Legal items are categorized by analyzing each item and asking, "*Does this item have any legal implications?"* Consider the item I_6: `DISCLOSE collected PII when required by law`; this item clearly provides information about a legitimate legal constraint and is thus categorized as a legal item.

Business items are categorized by asking: "*Does this item directly support the organization's business objectives?*" Consider the item I_{17}: `SELL aggregate information`; this item directly reflects business opportunities presented by the sale of gathered information and is thus categorized as a business item.

Technical items are categorized by asking: "`Does this item focus on domain-specific implementation details?`" Consider the item I_{18}: `PROTECT order information using SSL encryption technology`; this item is categorized as a technical item because it clearly focuses on a technical solution for protecting user information.

Contractual items are categorized by asking: *"Does this item focus on the relationship between a given organization and its business partners (e.g. third parties or business associates)?"* Consider the item I_{19}: `ALLOW affiliates to use PII for marketing and promotional`

`purposes`; this item impacts on the relationship between business partners and is thus categorized as a contractual item.

Social items are categorized by asking: "*Does this item address the relationship between a given organization and its customers?"* Consider the item I_9: `ALLOW customer to modify/remove their PII`; this item offers the user an opportunity to manage their relationship with the organization and is thus categorized as a social item.

Categorization of the health care privacy policy items involves differentiating between items according to the modularity categories of the framework. The analysis of the 39 privacy policies yielded 226 items, each of which was easily categorized according to the modularity categories. It is important to note that no items that overlapped categories were found.

Table 14 provides an overview of the modularity framework analysis and shows the number of hits for the modularity categories. These hit numbers are also broken down into sub-categories using major categories, and are classified as either privacy protective items or privacy vulnerability items.

Table 14: Summary of the Modularity Categories.

Modularity Categories	***Major Categories***	***Health Insur.***	***Drug store***	***Pharm. Comp.***	***Med. Inst.***	***Gen. Health***	***TOTAL Hits***
Legal	Vulnerability	4	7	1	2	5	19
20 (2%)	Protective	0	0	0	0	1	1
Business	Vulnerability	0	8	3	6	22	39
118 (11%)	Protective	6	15	3	8	47	79
Contractual	Vulnerability	8	29	9	9	54	109
182 (16%)	Protective	6	23	4	6	34	73
Social	Vulnerability	13	35	14	38	120	220
554 (50%)	Protective	29	84	38	32	151	334
Technical	Vulnerability	11	23	10	17	42	103
228 (21%)	Protective	12	27	8	13	65	125
TOTAL	Vulnerability	36	102	37	72	243	490
	Protective	53	149	53	59	298	612
TOTAL		89	251	90	131	541	1102

Next, each of the framework categories are discussed within the context of the analysis of Internet health care privacy policies.

4.6.4 Summary of Findings

4.6.4.1 Legal Category

The framework's legal category concerns privacy items and/or privacy obstacles that conform to or are permitted by law or established rules. Privacy policies must comply with the relevant legislation. Health care Web sites must adhere to more specific legislation pertaining to, for example, licensing and liability, malpractice laws, and other health care regulations such as HIPAA. Since the law is the most obvious influencer in the privacy policy and privacy management arena, the legal category is designated as the framework's outer layer, since these laws ultimately constrain the privacy practices of the inner layers.

In the study, half of the analyzed privacy policies contained provisions for sharing customer information with law enforcement agencies in the event of a criminal investigation or suspected illegal activity. However, this was accomplished using one of the three legal items discovered, specifically, item I_6, `DISCLOSE collected PII when required by law`. Furthermore, only 20 of the 1102 hits were categorized under the legal category. The majority of those were categorized as privacy obstacles.

Legislative approaches center on how governmental agencies can best write public policy to protect privacy and according to the theoretical sensitivity based on Section 2.3, the EU directives and the EU-recommendations, the legal items were expected to provide privacy protection. It was stunning to realize that these were in fact privacy obstacles. For example, item I_{20}, `DISCLOSE PII for tax purposes`, does not support privacy protection in any way.

4.6.4.2 Business Category

Section 2 has discussed the fact that values and beliefs must be included in any discussion of an organization's privacy policies. In an ideal world, organizations are objective and neutral; however, the values, beliefs, and interests of an organization may be in direct conflict with the values, beliefs, and interests of their customers and/or partners. Generally speaking, an organization's objectives are to create products or provide services while

maximizing profits. In some settings, that task may seem unrelated to values. However, in today's electronic commerce values, beliefs, and different interests are extremely relevant.

The framework's business category concerns enterprise objectives and activities of those engaged in the purchase or sale of commodities and/or other financial transactions. An organization's privacy policy is greatly influenced by its business objectives, and trust is an important element of successful business as discussed in Section 3.1. It is normally built on trust while in a social setting of face-to-face meetings. Engaging in business transactions on the Internet is a blind process so there is a need to strengthen trust in other ways. Trust is easy to lose but hard to gain; therefore, a privacy policy should directly reflect those principles that companies intend to provide. In particular, business objectives and practices often center upon how data is collected and transformed into information that ultimately becomes a valuable business asset: business knowledge.

For an organization to have an effective Web site, it should provide its users a protective and reliable vision. Additionally, it should tell users why the information is collected and how it will be used thereafter. Some organizations behave opportunistically and try to obtain as much value as possible from consumer data. For example, the use of data mining is an effective tool for finding hidden patterns and relationships in databases. Organizations are ready to sell this to third parties because more profit may be gained from the sale of such information today than in the past. This is primarily due to the ease of collecting such information combined with the recent occurrences with online businesses.

The framework's business category seeks to facilitate the process of evaluating these information practices as expressed in organizational privacy policies. Focusing on the business category allows privacy managers to consider the notion of general trust by exploring the privacy safeguard administration and management.

In the study, the share of business item hits was 11 percent. The weight of categorization was on protective, which reflects the business items as a positive trust indicator. The actual requirements expressed in a privacy policy are business items, but they have to go through a series of filters (e.g. legal). Furthermore, business items are motivated by the technical possibilities, social norms, and contractual norms of an organization.

4.6.4.3 Contractual Category

The contractual category focuses on the binding agreements that form the basis for information exchange between an organization and its third partners or business associates. Data and information exchange frequently occur between several organizations based on a set of reciprocity norms.

Using modern telecommunications and computing technology, organizations are able to easily share information regardless of geographical distance. Information and knowledge can quickly spread between organizations due to business relationships and contractual obligations. These inter-organizational relationships often become very political as organizations become influenced by the transactions and communications between them (Evans and King, 1999; Honeycutt, Flaherty and Benassi, 1998).

Contractual networks can generate new information when participants combine data elements together. These and many other new collaboration practices increase consumer vulnerability. Additionally, in their search for new ways to do business, certain companies have outsourced some of their functions. For example, information technology requires specialized and high competence, which is often cost-effective to contract outside of the organization. This implies the existence of increased vulnerability, because organizations must relinquish a certain amount of control to that beyond their own employees. As information technology-based activities are the primary internal functions concerning security, these are particularly important.

There are also many other contractual concepts to consider. For example, external links to other sites can help make a Web site's content more valuable to users (Heath, 1997), and informational content that is not directly generated by the company increases the objectivity of a Web site (Alexander and Tate, 1999). But according, the study of these kinds of practices may yield the item I_8: *ALLOW links to other sites whose privacy policy is different.* This item is categorized as a privacy vulnerability item.

The contractual category focuses on how information transfer and information use by external organizations affects consumer privacy. The relationship between organizations and how they cooperate was examined. There were 182 hits of items addressing the contractual category. This results in 16 percent of the total item hits from the 39 privacy policies. The majority of these contractual hits were categorized as privacy vulnerability items rather than privacy protective items.

4.6.4.4 Social Category

The framework's social category focuses on organizations and their users (or customers) in terms of how customers and companies interact and cooperate to exchange goods, services, and/or information. Thus, the social category reflects the relationship between the customers and the organization.

An example of a social interaction is the collection of information from Web site visitors. This social interaction is taken to an extreme when visitors are recognized as repeat visitors and subsequently greeted by name! Social category items differ from contractual items in that social items do not reflect any pressure or binding agreement between the consumer and the organization. If a user has the opportunity to make a choice about how his information is used, then the item is indicated as a social category item. Some of the most typical social category items are presented in Section 4.2.

Fifty percent of the 1102 item hits addressed the social category. More specifically, it 554 hits of social category items were discovered within the 39 privacy policies. These items were primarily categorized as privacy protective items rather than privacy vulnerability items. This implies that the organizations are aware of the importance of their relationships with customers and try to support customer needs to protect privacy. The majority of those protective items also supported the balanced privacy model.

4.6.4.5 Technical Category

An open network, such as the Internet, contains several access points that are potential targets for hackers to penetrate an organization. With many technical problems and threats, we are becoming depressingly aware of the extent to which our privacy depends on the proper functioning of security systems. As information systems have become linked, system security has come to depend more heavily on various forms of secrecy or logical security (Thompson, 2001, p. 16).

Security measures are necessary in all organizational networks, and the items addressing such measures belong to the technical perspective. Technological approaches take into consideration how informational privacy can be best protected through 'engineered' means. For example, to protect identifiable information maintained at a Web site, a company might develop a secure password system and encrypt data to protect the information transmitted from one computer to another or through a network.

IT practitioners need to focus on the technical measures necessary to provide a secure information technology environment that effectively protects consumer privacy. Such measures should support information technology processes inside the organization, data transfer across the Internet, and security features on user systems. Additionally, technical viewpoints of the organization should be embedded in the design, implementation, and use phases of information systems. Although the information being delivered is more important than the delivery vehicle, this category is important because security mechanisms are used to shield the information (in transit and in storage) from unauthorized users. The technical category items address security across an entire transaction.

The vulnerability of information being exchanged is partially dependent upon a transaction's context. Although a message might contain highly sensitive information (e.g. health-related personally identifiable information), it is important to consider the form of the information as the way in which it is delivered. If messages are securely encrypted using the most advanced techniques then customers can expect a high level of security and privacy. This in turn invites a high level of trust within the organization as well as perceived trustworthiness from those outside the organization.

In the analysis, 228 of the total observed item hits (21 percent) were technical category items with over half of these being protective items and less than half being vulnerability items. This balance was expected since technology is used to protect users while also supporting the organizational goals of increasing and maximizing profits.

4.6.5 Conclusion

Some proposals and suggestions for how to deal with privacy issues involving information technology fall into one of two types of categories: proposals that are technology-based and those that are legislation-based. It would seem that neither of the two categories provides a fully adequate solution to the privacy issues. Privacy management must be evaluated from several categories within an organization; these categories primarily include legal constraints, technical measures, business rules, social norms, and contractual norms. The framework presented in this section addresses those modularity categories and aims to provide a conceptual framework for responsible and efficacious privacy management.

The legal category concerns legislation that must be adhered to and which constrains the other four categories. Legislative approaches center on how governmental agencies can best write public policy to protect privacy. The legal items were expected to provide privacy protection. It was stunning to realize that these were in fact privacy obstacles.

The business category reflects the fact that business objectives and practices often pass through legal (and in some cases also technical) filters. Business objectives and practices center upon how data is collected and transformed into information that ultimately becomes a valuable business asset. The weight of categorization was on protective, which reflects the business items as a positive trust indicator. The business category involved in e-Health has items that are motivated by social and contractual norms that further restrict the organization.

The contractual category focuses on the binding agreements that form the basis for information exchange between an organization and its third partners or business associates. The majority of the contractual hits were categorized as privacy vulnerability items rather than privacy protective items.

The framework's social category focuses on organizations and their users (or customers) in terms of how customers and companies interact and cooperate to exchange goods, services, and/or information. These items were primarily categorized as privacy protective items rather than privacy vulnerability items. This implies that the organizations are aware of the importance of their relationships with customers and try to support customer needs to protect privacy.

The technical category offers tools and techniques that support, and restrict, the manipulation of consumer data. According to the study, technology is used to protect users while also supporting the organizational items of increasing and maximizing profits.

The process of allocating (or classifying) policy items to each of the modularity framework categories refers to the capacity to view things in light of their true relationships or relative importance. The modularity category scheme seeks to help the privacy manager maintain a holistic view of privacy within the context of their organizations in tandem with how those categories constrain and influence information practices. Privacy policy and privacy practices must be considered within a framework that recognizes the role and influence of the modularity categories.

When employed to create a privacy policy, the modularity category scheme will ensure that privacy managers and officers adopt a more holistic view of the organization's information practices. Privacy policies should express

organizational values and beliefs that relate to organizational success factors, as well as customers' privacy concerns that are reflected directly through their thoughts and actions. The scheme demonstrates that the framework also provides a useful modular basis for analyzing and comparing privacy situations. The modularity categories offer a foundation for reasoning about the health provider and Internet privacy policy and privacy management from the viewpoints of the balanced privacy model, which is discussed in the following Section.

4.7 Towards an Approach to Managing Privacy Policies

> *"Technological change cannot be stopped –*
> *only directed (if we are lucky)."*
> *(Pearson, 2003).*

The ability to provide differentiated, consistently superior customer service on the Internet will be crucial to the survival of health care companies, but the findings of this study submit that health providers' Web sites are still at relatively early stages in their privacy issue evolution. In addition, previous studies and practices (i.e. regulations, directives, laws, and seal programs) have taken a sweeping approach that neglects the important distinction among the different interests affected by computerization and does not acknowledge the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings. The older studies do not provide sufficient concept to answer the questions, such as: how can we balance customers' interest in privacy with the benefits of having so much more data? And how would it be possible to balance the rights of customers to privacy against the desire of companies to use this technology to improve their marketing and to better target their products to the interests of customers? All these shortfalls may be partly due to the speed with which many companies have established an Internet presence.

When customer demands continue to increase and the availability of informational and interactive Web site content continues to proliferate, the bar for acceptable performance by health providers will continue to rise. In that situation, very strict normative privacy regulations according to the balanced privacy model mean that customers are not able to get satisfactory health services. The industry in the U.S. has vowed to self-regulate, but privacy

practices of the Internet are underdeveloped in general. The empirical part of the study points out the discovery of numerous examples of practices that increase the vulnerability of customers. Most sites do not meet fair information practices – such as providing adequate privacy notice, giving users some control over their information, and holding business partners to the same privacy standards. In addition, obvious and visible privacy practices can be found, but insidious and invisible privacy practice management can also be found – anyone who does not want to be misled by hidden tactics has to read all privacy policy statements carefully. In addition, the lack of terms and content standardization creates problems for people that want to compare the privacy policies of different organizations before deciding which organization to entrust their personal identifiable information to. Although the most significant facts about the privacy seal program are trust, ease, and visibility, the study results indicate that the privacy policy seal does not mean the reduction of uncertainty and risk for the health Web site user without the user first having to read the privacy policy statement. Privacy seal programs might have the potential to provide that assurance, but they do not necessarily mean full privacy protection and security.

We have concluded that the development of privacy policy is a diverse task and despite their underlying importance to the functioning and organization of e-commerce, the optimum result has not yet been achieved. It is relatively easy to set up a Web site, but far more difficult to create a web-based business model. In the theoretical part of the study, the author presented a more developed business model for e-commerce, the balanced privacy model, where customer privacy (the Privacy-on-Demand function) was related to the function of service (the Service-on-Demand function). Since the balanced privacy model seems to be a suitable business model for e-commerce, we need methods and techniques to construct it. In that setting, the major category scheme (i.e. protective and vulnerability category) and the visibility category scheme (i.e. visible and invisible category) have a central role. Additionally, we have learnt that privacy rules stem from, and are constrained by, the different modularity categories: legal, technical, business, social, and contractual. All those category schemes provide properties and entities for the proposed privacy process model that is presented in the following sections. It is aimed at helping corporate privacy managers to consider the different implications of the privacy policies and practices for which they are responsible.

4.7.1 Introduction

So far we have pointed out that the conceptual uncertainty generated by many changes affects our understanding of the privacy situation. In the context of e-commerce, this is partly a technical issue because information systems rapidly introduce new possibilities, but it has many other consequences as well. Even standard operating procedures can shift in meaning as they become informationally-enriched and regularly produce policy vacuums. Additionally, in situated action the actor acts intentionally and competently without a ready-made plan, letting the awareness, interpretation, experience, and overall goals have an implicit impact. This is not to say that we can't achieve conceptual clarity or formulate and justify reasonable policies using different tactics and the balanced privacy model.

The task of drawing up a comprehensive privacy policy governing all organization activity would be possible if no changes in organizations or services would be required. In that situation, a detailed privacy policy of Internet service could be laid down for fairly long periods and closely adhered to. Considering the presented theoretical frameworks and empirical studies, it is understandable why organizations can't operate that way. The Internet enables more functional and complex electronic commerce applications and their solutions and improvements can threaten or support ethical objectives. When new solutions are adopted, an organization's security policy and privacy policy must be revisited and oftentimes revised to respond to policy conflicts introduced by these new solutions. It is, perhaps, worth stressing that many problems arise as a consequence of change. As long as all things continue as before or at least as they were expected and planned to, no new needs arise which would require a decision on the use of personal information and subsequently there is no need to form a new privacy practice. There are no policy vacuums in such situations.

KPMG's Internet Maturity Model suggests that Web sites go through four distinct
stages as the firm's electronic commerce strategy evolves – marketing, publishing, transactional, and interactive. All of these stages need their own privacy practice consideration. The changes between stages are probably not very fast and organizations have time to review their privacy practices accordingly. However, within the Internet business, minor privacy-related decisions are required at short intervals, for example, when a new customer service function is about to be implemented. In addition, once the customer service has been implemented, the rest is not only a mechanical issue. We

have learned that privacy issues are much more than information systems. Information systems potentially change important organizational dimensions, including the structure, culture, power relationships, and work activities. There are many possible amendments involved in changed and informationally-enriched standard operating and articulation work processes. “Informational enrichment can also affect ethical and legal practices and concepts.” (Moor, 1998, p. 16).

As determined by the character of the Internet service, there is much to be changed in adapting to new business matters and the changing circumstances of environment. As in the case of cognitive limits to consistent behavior, the first radical change of attitude after September 11th does not mean that the rational choice approach has to be relinquished. Rather, we should look at rationality with a broader mind. Individuals are super-rational in the sense that, in general, they are able to guard themselves against a certain threat (Frey, 2001). In particular, it is not automatic that if one allows the future to be unknowable before its time and undetermined by past events, one has to necessarily jump to the polar opposite from perfect foresight and proclaim that we can say nothing about anything (Earl and Kay, 1985). The oracular perspective certainly does involve rejection of the notion that privacy managers should seek to make single-line predictions of what will happen. However, it does not deny that we might be able to contribute to the process of policy formation by providing insights into the range of things that could happen. An inability to specify or define permanent privacy policy does not mean that the organization cannot draw up sufficient visions of privacy issues in advance. A privacy manager who has accepted the oracular perspective can contribute to the process of privacy policy formation in a variety ways, all of which have a good deal in common with the functions served by those strategic thinkers in large corporations whom Jefferson (1983) has characterized as “*scenario planners*”. The privacy manager can actively attempt to highlight the areas of uncertainty in the existing structure of the whole Internet service. He/she may have some appreciation of what a disaster organization might have to cope with and what opportunities they might be able to grasp (providing they make advance preparations) if they implement particular changes of privacy practices. Secondly, he/she can actively attempt to propose improvements to the Internet service, business processes, and privacy practice so that they are better able to cope with dangerous threats if they materialize. Thirdly, he/she can attempt to discover ways of modifying or eliminating the incidence of surprises in the ICT architecture, business infrastructure, and environment.

Cross (1982) characterized the vision of uncertainty via a "*non-diagram*", the position of those who emphasize the unpredictability of events. The "*non-diagram*" shows a point in space depicting the current configuration of variables, with arrows leading off in all directions to depict what may happen next. Based on the privacy policy study, we can submit that the privacy manager seeking to thoroughly undertake all those tasks in the rapidly evolving Internet world is likely to be in the "*non-diagram*" situation, where he is unable to make a choice between rival possibilities. Additionally, a privacy manager should anticipate privacy situations with which customers will have to deal, but if privacy policy expresses all the alternatives that may happen, it might begin to resemble an everlasting story. One could well imagine that a customer might end up "*failing to see the forest for the trees*" if he/she sought to arrive at conclusions about privacy issues and practices of the Web site. It is important to remember that the prospective customer has a direct impact through the whole e-market. Web sites should be set up to encourage business, not to preclude it. If prospective customers cannot easily find what they are looking for on a health care Web site, they may move on to find another site that makes its informational and interactive content more apparent.

A prominent and promising strategy employed for coping with turbulent environments is to devise methods of localizing and limiting the change posed by external demands, even if the source or form of the impulse cannot even be approximately specified in advance. If individual sub-systems can be decoupled from the overall system without threatening the latter's integrity, then this may form the basis of system design in turbulent environments (Earl and Kay, 1985, p. 40). Following Simon (1969), Earl and Kay expected that after a period of environmental turbulence, the surviving systems would be found to be those that had exhibited a good deal of decomposability.

4.7.2 Different Tactics of Modularity

According to the balanced privacy framework, accurate privacy policies must try to cope with the inherent uncertainty of the future, and therefore the privacy manager may face a situation where one useful method could be to design privacy policy so it is possible to make the change of policy in a flexible manner. If we evaluate the privacy situation from the company's perspective, the organic privacy policy, which is characterized by continual adjustments, tends to be more appropriate for a rapidly changing environment.

In contrast, if evaluation occurs from the customer's perspective, possible changes may weaken the customers' privacy protection. In that situation, the privacy manager may feel that it is desirable to try to and understand behavior at the organizational level, where uncertainty most likely occurs and then choose the tactics accordingly. It seems practical that the privacy manager would try to classify the situation in terms of key characteristics – for example, stability/turbulence, static technology/dynamic technology, high sensitiveness/low sensitiveness – thus considering ways in which the organization might seek to cope with different privacy situations.

Based on the privacy policy study, the modularity category scheme gives uncertainty many separate meanings from the customers' perspective, and these meanings need to be distinguished for clearance and for the reasons of different tactics. The first type of uncertainty, which is called *legal uncertainty*, arises when a radical change of relevant legislation occurs, for example, the implementation of HIPAA. The second type of uncertainty, which is called *business uncertainty*, concerns enterprise objectives and activities of those engaged in the purchase or sale of commodities and/or other financial transactions. The third type of uncertainty is called *contractual uncertainty*. This concept focuses on the binding agreements that form the basis for information exchange between an organization and its business partners, for example, when companies have outsourced some of their functions. The fourth type of uncertainty, which is called *social uncertainty*, focuses on organizations and their users or consumers in terms of how both kinds of stakeholders interact and cooperate to exchange goods, services, and/or information. The final type of uncertainty, which is called *technical uncertainty*, arises with many technical problems and threats. Customers are becoming aware of the extent to which their privacy depends on the proper functioning of security systems.

Next we propose how a privacy manager is able to manage uncertainty issues using different tactics. The minimum requirement of the privacy policy is that it must comply with the relevant legislation. It is supposed that these kinds of normative changes won't happen often. If we consider the empirical part of the study and the balanced privacy model, legal issues can be managed according to the long-term vision and there seems to be no need for flexibility. One of the most important variables that affect the boundaries between company and customer is the company's business strategy, which is included in the business category. According to the privacy policy study, business objectives and practices often center upon how data is collected and transformed into information that ultimately becomes a valuable business

asset: business knowledge. Although there are many definitions of business strategy, most agree that strategic decisions conform to several characteristics: they affect an entire firm or a significant portion of it ("*a strategic business unit*"); they are made by top level firm or divisional managers, and they are long-term in nature (Langlois and Robertson, 1995, p. 17). According to the empirical part of the study and the balanced privacy model, business issues seem to need some flexibility. Basically, the privacy manager approach to privacy policy and privacy protection can follow long-term vision especially in the case of business and legal categories. From the customer's perspective, long-term tactics entail predictability for privacy issues, because overreactions of radical change can be avoided and at least balanced using a predetermined long-term strategy.

According to the study, the changes involved in the contractual category can make customers very vulnerable. Those changes reflect directly on the customers but they also affect business strategies. According to the empirical part of the study, they seem to be partly long-term and partly short-term in nature. They are called, therefore, mid-term issues. Based on the balanced privacy model and the privacy policy study, they need flexibility. The changes concerning the social category seem more likely to be short-term in nature than long-term according to the analyzed privacy policies. Social issues need a lot of flexibility, which is the core concept of the balanced privacy model. An approach to technical matters should follow in the nature of short-term vision, because it is very likely that new threats of security and privacy invasion will materialize after new information and communication technology becomes widespread and invaders learn how to subvert it. The best security practices, as they are understood at the time, should be embedded widely in organizations. Revisions of security precaution measures are needed regularly. New threats take time to catch up with the technology and exploits, but over time, the best practices of invaders emerge (Prince, 2001). Employee awareness programs and technology-based solutions are an effective means of reducing the risk in those cases and, thus, the short-term tactic entails protection for customer privacy.

In taking a risk-based approach, privacy managers treat privacy issues as secrecy matters. The primary advantages of a risk-based approach reside in its conceptual clarity. The value of protecting information derives not from a Warren and Brandeis-style right to privacy, but from a company's duty to protect its customers from very basic forms of personal harm (Rachels, 1975; Bok, 1983). For two decades specialists in risk analysis promoted the idea that measuring the probability and value of an unwanted event could be given over

wholly to technical analysis, and that ethical or political questions must be confined to the acceptability of risk as measured in these technical terms (Thompson, 2001, p. 17). Paul Slovic, a former president of the Society for Risk Analysis, has written that, "*In sum, polarized views, controversy, and overt conflict have become pervasive within risk assessment and risk management*" (Slovic, 1999, p. 690). There is a legitimate concern that the risk-based approach would simply import this conflict into the privacy policy evaluation and formatting process. If that were the case, we might be better off leaving these security issues to be framed in terms of technical concepts. Analyzing technical matters as the security issues means a step in the direction of clarity and accuracy.

Privacy protection that treats all privacy issues as secrecy matter might cause harm to customers and their interests. Those who view privacy issues simply as the chance of injury, damage, or loss neglect the way the role that voluntariness, consent and intentionally in the balanced privacy framework. The balanced privacy model offers a systematic means to resolve the issues at hand. It provides us with a procedure for addressing privacy concerns involving electronic commerce business. The model allows customers to opt-in or opt-out of different features and functions as discussed in Section 3. One strength of the balanced privacy model is that it requires a company to openly state what the parameters of a private situation are so they will be "*completely public*" and presumably known to all those in or affected by a situation. The modularity category scheme provides a construct to consider the privacy interests of customers against the economic interests of businesses in a flexible way using different tactics. As a summary of the preceding discussion, the different possible tactics of companies, the customers' need and the form of balanced line (as presented in Figure 5) are presented in Table 15.

Table 15: Tactics and Needs for the Modularity Category.

Category	***Company's Tactics***	***Customer's Need***	***The Form of Balanced Line***
Legal	Long-term	Fixed	Direct ($BL_{1)}$
Business	Long-term	Flexible / Fixed	Curve (BL_2) / Direct (BL_1)
Contractual	Mid-term	Flexible / Fixed	Curve (BL_2) / Direct (BL_1)
Social	Short-term	Flexible	Curve (BL_2)
Technical	Short-term	Fixed	Direct ($BL_{1)}$

In a privacy process, a privacy manager may exploit the adaptability features of modular design. He is able to use the modular category schemes to build a suitable modular view of possible changes. It offers an opportunity to

probe each modular category as an entity, but also as a part of the larger holistic view of the privacy situation. Some suitable tactics seems to be long-term for predictability and clearance, and some useful tactics are short-term for security and flexibility. Based on the balanced privacy model and modular categories, we have a clearer understanding of which considerations and tactics are relevant for setting up a privacy policy, but we have not yet determined what kind of privacy process is suitable for the organization to adopt.

4.7.3 Layered Privacy Model

This section presents the layered privacy model. The model gives the basic construct for the privacy process, the aim of which is to improve the efficiency and effectiveness of privacy practices. The strength of process thinking is in the self-reflection of the organization: how can we in our organization improve the competitiveness and effectiveness of our activity (Klimas, 1997; Hammer and Champy, 1993). The commitment to improve the efficiency and effectiveness of privacy practices inherent in the process thinking indicates that there are several ways of doing a given thing. Only then does it make sense to argue that one of them is better than another. Additionally, it is obvious that privacy practices can be accomplished in many ways, and the study findings submit that health providers' Web sites are still at relatively early stages in their privacy issue evolution. In order to protect their privacy, a relatively small number of savvy customers are devising their own "opt-in" policies and deciding that some Web sites are not worthy of getting their personal information and most users do not use the available privacy protection tools, perhaps because they are unaware of how Web sites work and how existing technologies can be deployed to protect them (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 3).

The conditional matrix presented by Strauss and Corbin (1990, p. 161) seems to be a powerful analytic tool for capturing the many categories and properties bearing upon a privacy practice. By tracing the conditional and consequential paths through the different matrix levels, it is possible to determine which levels are relevant. The ONION model (Kortteinen, Nurminen, Reijonen and Torvinen, 1995) also offers a useful approach to the privacy process, although the model was originally developed for evaluating information system performance. "*The ONION model is hierarchical. The origin of the hierarchy is in the conditionality: evaluation at one level requires*

the acceptance of the next larger context to the object of evaluation." The model comprises the design idea of Saarinen (1956): "*Always design a thing by considering it in its next larger context – a chair in a room, a room in a house, a house in an environment, an environment in a city plan*". The idea of ONION model is to climb through the ONION hierarchy while evaluating the activity at the same time. The basic model is presented within four levels: individual, group, organizational unit, and enterprise[96] .

In the economics context Earl and Kay (1985, p. 38) have also pointed out the useful idea of a layered structure that considers turbulent environments. "*Even though their individual events may be unpredictable, different kinds of turbulent environments may display particular regularities of patterns, signaling the need for appropriate system design of procedure if the decision maker is to operate and survive in his own particular turbulent environment*". So although the economist may be unable to predict the unpredictable, at a higher level of abstraction it may be possible to expect the unexpected, as Boulding (1968) has suggested.

The combination of the conditional matrix, the ONION model, and the ideas by Earl, Kay and Boulding offer a constructive model for the revision and assessment of privacy policy. It is called *the layered privacy model from now on.* The layered privacy model may be represented as a set of levels, one inside the other, each level corresponding to different aspects of the organization as presented in Figure 20. The outer levels contain those conditional features most distant to the action/interaction; while the inner levels pertain to those conditional features bearing most closely upon an action/interaction sequence. Privacy situations at all levels have relevance to the privacy process. Even when studying a privacy situation that is clearly located at the inner part of the matrix – the action/interaction level – the broader levels of conditions will still be relevant. For example, workers in any interaction bring along the attitudes and values of their national and regional cultures, as well as their past experience.

To maximize the generalizability of the layered privacy model as an analytic tool of privacy practice, each level is presented in its most abstract form. As we have noted, each privacy situation possesses the properties of time and place. The researcher needs to fill in the specific conditional features for each organization level that pertain to the chosen area of investigation. Items to be included would thus depend upon the type and scope of the

[96] Järvinen (1999, p.22) presents the information system evaluation model within ten layers in the university central hospital context.

category scheme under investigation. It is possible to study privacy practices at any level of the model. For example, one might study visibility category items within a customer interaction level, or business category items in the organizational decision-making level, or legal category items in the level of data transfer between countries. One important point to always remember is that regardless of the level within which privacy policy statement is located, that privacy practice will stand in conditional relationships to levels above and below it, as well as within the level itself.

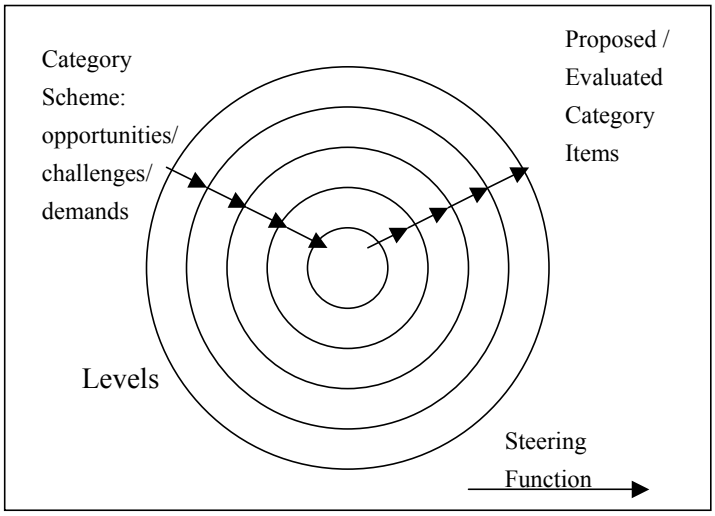

Figure 20: Layered Privacy Model.

It is proposed that privacy policy criteria on each level must be drawn from the opportunities, challenges, and demands of the current category scheme. Privacy practice is evaluated and revisited on each level according to the local criteria of 'a good performance'. In this way privacy policy is anchored and becomes relative to the view taken on each level. The evaluation criterion of privacy policy can be given on another level and it gives us consolidation. Using the layered privacy model, a privacy manager is able to form/revise privacy policy statements that are appropriate in each level but also sufficient for the balanced privacy model.

The empirical part of the privacy policy study points out that many organizational levels are needed. Privacy policy statements cover many kinds of business processes, which are located in varied organizational levels. The next proposals are based on the structure of the layered privacy model and the analyzed privacy policies. The outermost level may be thought of as the international level. It includes such privacy matters as international politics

and techniques, governmental regulations and directives (for example EU-directives), culture, and values. The second level may be regarded as the national level. Its features include national politics, governmental regulations (for example HIPAA), culture, history, values, and economics. Next comes the business segment level, which includes all the above privacy matters as they pertain to the business area. Each business segment has its own features that give it singularity (for example, health care). Moving inward, we find the institutional and organizational levels. Each will have its own structure, rules, and privacy issues. Still another level represents the sub-organizational and sub-institutional level. This would include such peculiar features as the part of the health care ward, or the sub-location within a larger location where the privacy study is taking place. Then, we reach the collective, group, and individual level. This level includes knowledge and experiences of persons, as well as those of various groups (special interest, professionals, and scientific). Later, the interactional level is reached. In this context, interaction refers to people doing things together or with respect to one another with regard to a privacy practice and the business processes that accompany doing things. Even things done alone, like managing customer information using a computer, require interaction in the form of self-reflection, and contact with others to obtain, for example, technical support. Interaction is carried out through such interactional processes as negotiations, emails, computer systems, discussion, and self-reflection. Reaching the center of the layered privacy model, we find action: situated actions and practices of standard operating procedures. This level represents the active, expressive, performance form of self and/or other interaction carried out to manage privacy practices. Action is carried out through action processes. These combine with interactional processes to complete the picture of action/interaction (Strauss and Corbin, 1990, p. 162).

4.7.4 Steps of the Privacy Process

This section adapts the layered privacy model for different category schemes and the balanced privacy model for the proposed privacy process. The privacy process is presented in the form of nine sequential steps. The privacy process can be accomplished in every organizational level of the layered privacy model focusing on each modularity category scheme. In that case, the privacy manager delimits the scope by considering the matters of that level and current category. The steps involved in the privacy process are the same when

focusing on the privacy matters as a whole or per one modularity category scheme, and they include:

1. Delimit the scope of privacy focus by finding out the actions that affect or are affected by privacy issues.
2. List the corresponding privacy actions on every level.
3. Describe the privacy actions in work-oriented terms.
4. Evaluate every privacy action using the major category scheme (the protective and vulnerability items).
5. Elicit the probable causes of eventual privacy deficiencies or deviations.
6. Revise privacy actions using the balanced privacy framework.
7. Express privacy policy clearly using privacy policy keyword terminology and the major category scheme (i.e. protective and vulnerability items).
8. Design Web sites practices according to the balanced privacy framework using the visibility category scheme.
9. Design Web sites according to the balanced privacy model using the interactivity properties of the Internet.

Steps one thru six are mainly targeted to support the privacy process for internal reasons. Obtaining a clear conception of the situation upon which to evaluate and/or formulate privacy policy is the logical first step in the privacy process. There are too many situated and standard actions in the organization and informationally-enriched processes to thoroughly consider them all, and therefore it is important to focus and concentrate mainly on the actions which affect or are affected by privacy issues.

Chronologically, a privacy manager's uncertainty about the appropriate policy may precede and motivate the search for conceptual clarification, and the list of potential benefits from process thinking results from making work and privacy practices visible. Organizational routines and norms direct employees' actions, resulting in cumulative privacy policy utilization to support organizational goals, but by doing that they may also constitute a privacy threat to customers. The privacy manager should be aware of the corresponding actions on every level of the organization, and therefore it is important to list the corresponding privacy actions on every level. Thus, this is the first step to make invisible and tacit privacy practices visible.

The privacy manager should describe privacy practices in work-oriented terms, which provide a means to guide communication among different partners and employees. The co-workers have to give words to various aspects in their work situation, in particular to how privacy actions are done in the community. This kind of self-reflection as such may be useful in most

organizations regardless of the method used and the explicit result received. The joint modeling processes may lift possible variations in privacy practices among employees to the forefront. The evaluation of a privacy policy may thus require close examination and perhaps refinement of employees' value (Smith, Milberg and Burke, 1996). Awareness of such differences is likely to harmonize the privacy practices even if the self-reflection would not lead to the formulation of uniform privacy practices. In addition, Ansoff (1979) argues that many potential strategic surprises could be avoided if organizations develop techniques to recognize and act on early hints and clues from the environment. This view seems to be equal to privacy practices (Prince, 2001). The privacy manager might be more confidently able to prevent a privacy problem when listening to weak signals where privacy issues are important and would thus be able to act appropriately.

The privacy manager should use the major category scheme to evaluate the protective and vulnerability items of every action in every level of organization. Privacy protective items relate to the desired protection of the customer privacy practice, whereas privacy vulnerability items relate to existing threats to customer privacy. On each level, privacy practice is evaluated according to the local criteria of good privacy practice. Evaluation on one level requires the acceptance of the next larger context. After evaluation, the privacy manager should elicit the probable causes of eventual privacy deficiencies or deviations. It may be possible to convert vulnerability privacy issues into protective privacy issues, and therefore the privacy manager should revise insufficient privacy actions using the balanced privacy framework.

One result of privacy process steps one thru six should be a full description for the organization's privacy practice, which is mainly targeted for internal use only. The assessment of privacy practice is definitely a demanding field of ethics which requires more that routine application of principles, and the consideration of the privacy situation needs flexibility as discussed earlier. Considerable interpretation is required before an appropriate privacy policy can be formulated and justified. Privacy practice evaluation may lead one back to further conceptual clarification and then on to further policy formulation and evaluation. Eventually, some clear understanding and justifiable privacy policy should emerge. Of course, with the discovery of new consequences and the application of new technology to the situation, the cycle of conceptual clarification and privacy practice formulation and evaluation may have to be repeated on an ongoing basis.

The last three steps of the privacy process are focused especially on customers' interests. They are also targeted to support organizations to design Web sites that allow customers to make their decisions according to the balanced privacy model. The values, beliefs, and interests of an organization may be in direct conflict with the values, beliefs, and interests of their customers and/or partners. The company should, therefore, express their privacy practice clearly and openly. It should be reasonably understandable and designed to call attention to the nature and significance of the privacy situation. It is important that a privacy practice is available to customers without requiring extensive searching and reading processes. Web site design is also critical because Internet users are in control of which sites they go to and are probably less inclined to revisit Web sites that are not trustworthy.

According to the study, Web sites' privacy policies focus on different privacy practices and express the same privacy practices using different terms, which require end users to calibrate their understanding of different Web site policies, thus imposing a tremendous (and unfair) burden on the end user. Additionally, previous studies point out that not all consumers can (or are willing to) take time to read and understand privacy policies. In that situation, there is a need for organizations to standardize the way in which they focus on and express their privacy practices. It is an important matter because many analyzed privacy policies contain technical and confusing language (i.e. unnatural language) that makes it difficult for the users to fully understand what they are agreeing to. One target of a successful privacy process is to make privacy policies more clear and understandable, benefiting both the company and the customer. Major category schemes would facilitate the use and the development of privacy policy keyword terminology (Table 3). The list of formally defined keywords provides a useful and extensible vocabulary because they standardize what different policies express with different terms. A standard vocabulary and the use of majority categories would be beneficial for customers and companies. These practices would enable the formulation of privacy policy that is reasonably understandable and designed to call attention to the nature and significance of the information in the notice. These practices would also enable the formulation of privacy policies that are able to communicate more privacy practices of the company. For example, the names of company privacy managers and the provision of informational content, such as the times when the privacy manager is available, would be helpful to prospective customers. This kind of practice signals that the organization has the necessary expertise and resources to support privacy management and the

existence of these issues encourages trust. This type of information was noticeably lacking on all of the health care Web sites that were evaluated.

The visibility categorization scheme incorporates several sub-categories that impact on privacy policy content as well as privacy management practices and operational system requirements. The privacy manager should encourage Web site designers to design Web sites according to the balanced privacy framework using the visibility category schemes. For example, many changes imply a requirement for an up-to-date privacy policy, meaning that a privacy policy change since the customer's last visit should be available to the customer without an intensive search and reading process. The proposed categorization scheme is effective for examining how privacy policy statements and their respective system requirements may be apparent to a consumer without the consumer first having to read the privacy policy statements. The contribution of the categorization scheme is primarily intended for software engineers, policy makers, and consumer advocates.

The proposed last step is to design Web sites according to the balanced privacy model. By converting the lean media of a privacy policy into a richer mode using the interactivity properties of the Internet, it becomes possible to make privacy practices clearer to customers, enabling them to choose their own preferences and make more informed decisions concerning whom they entrust their personally identifiable information with. Sufficient privacy management of the balanced privacy model allows customers to opt-in or opt-out of different features and functions.

Next, some proposals are made concerning what kind of possibilities the balanced privacy model entails. As mentioned earlier, site security and privacy issues continue to be a major concern for Internet users, and therefore the privacy policy should be consistently available, with the date of the latest revision clearly posted. The study pointed out that the revision date usually appears at the bottom of the privacy policy page. A simple, yet possibly effective strategy would be for Web sites to display the revision date at the beginning of the privacy policy, so users can easily find it. It would be even better if the revision date were also displayed on the homepage of the Web site supporting the visibility category. However, the revision date does not sufficiently describe the type of change that occurred. If changes are unspecified, they are almost uncontrollable to the user, and therefore the practice does not support the balanced privacy model sufficiently. If the user has to read the whole privacy policy every time and compare between the new and old, it is not necessarily user-friendly. However, all health care Web sites evaluated were not making an effort to alleviate this concern for visitors. Basic

site navigational tools like an internal search engine for privacy policies could not be found on most of the health care Web sites. According to the balanced privacy model, it would seem to be the responsibility of the organization to inform customers about the change of privacy policy, and not leave it up to the customers to discover it for themselves by studying the matter every time they visit the Web sites. All involved consumers need to be told explicitly that information about them is being used in new activities, since it would not be reasonable to expect the average consumer to be aware of new practices. If a company makes any changes to its privacy policy, the practice should let the customer know the effective date of the changes and provide a mechanism for the customer to understand what has changed. The mechanism should not only consider the previous visit of the user but also take note of the difference between the new and previous situation by showing the changed fragments.

A proposal concerning the data mining process, which in many ways is compatible with the balanced privacy model, is presented by Cavoukian (1998, p. 13-14). It would essentially grant consumers three choices: (A) Not having their data mined at all; (B) Having their data mined only "*in-house*"; (C) Having their data mined externally as well. Concerning privacy policy change, which can of course consist of data mining as a new practice, these other choices are also found: (A) The consumer does not agree with the new practices at all and demands that their personal information be deleted; (B) The consumer wants their personal information frozen at the current state of consent; and (C) The consumer agrees to the new practices. Privacy policies should provide assurance that previously gathered data won't be used in any new way before consent of the customer.

According to the balanced privacy model, i.e. the Privacy-on-Demand and Service-on-Demand functions, it is important that consumers be given the opportunity to decide what information is to be used and whether it may be used for new purposes after changes of privacy policy. Therefore, there should be an option that allows the customer to accept new use of old data or not. If customer does not accept the change, then the customer should be able to remove all data, update it, or freeze information usage at the level of the old privacy policy. If an old customer does not accept the new privacy policy at all, then customer status should be restored as a new customer and old data should be canceled.

When informed about the details of new practices, many consumers would perhaps be inclined to choose option A and elect not to participate in the company's processes at all in the future. Some consumers, on the other hand, elect to have their personal information used in older ways, because they are

used to getting services based on current information and practices, provided that they can be assured that information about them would not be used in new ways. Other consumers might elect option C and consent to their information being used in new ways, probably because of certain perceived new benefits they might receive. Some might see an advantage in the fact that their personal information is disclosed to third parties and unlimited uses of their consumer data by other organizations if it resulted in their receiving more directly targeted offers related to their specific consumer interests from other business partners. Information systems can help companies pinpoint tiny target markets for these finely customized products and services – as small as individualized "*markets of one*", rather than the general-purpose forms of "*junk mail*" that many consumers receive. Although relatively few consumers might be inclined to choose option C, the important point here is that through explicit and open notification and the opportunity to choose different alternatives, consumers could have a greater say or choice regarding how information about them is being used. Under an open and explicit notification practice of privacy policy change, consumers could negotiate with the organizations with whom they conduct transactions regarding new practices. If consumers select either of the above options B or C, they could enter into an ongoing dialogue with organizations, but option A means that dialogue is halted. The management of versions enables individual consumers to decide on a case-by-case basis exactly how much and what kind of information about them they are willing to permit a business to use. If there were certain incentives for customers to give consent for new use of information, such as more exact information, better offers, or rebates on the purchase of items for instance, some consumers might elect to participate in new practices and choose rich service function. Whether a customer chooses option A, option B, or option C, he or she can deliberately make an informed choice concerning new use of old and new information about himself. The interactivity properties of Internet technology give us an efficient manner to deal with the proposed practice of the balanced privacy model.

The Internet can be used to build closer but also more trustworthy relationships with customers. The balanced privacy model requires data management of the company for the reasons of effective privacy management. Customer data can be labeled with additional information, such as the privacy policy version, once user consent is obtained. This kind of practice provides the company with the opportunity to use old knowledge and new information effectively, but also in a trustworthy manner as the balanced privacy model proposes.

The balanced privacy model creates many possibilities to manage privacy practices so that the customers can make the most convenient choices in terms of their own needs and values from the alternatives, also over cultural boundaries. The findings from the study of Singh, Zhao and Hu (2003, p. 75) points out that the Web is not a culturally neutral medium. Instead there are significant differences in the depiction of local cultural values on the Web. This dissertation has discussed the thought that the concept of privacy has a distinctly cultural aspect – some cultures may value privacy and some may not. What one user considers a privacy invasion may be a valued feature or service to another user, which is the core idea of the balanced privacy model. Research in the area of cross-cultural perceptual categorization and information processing (Detweiler, 1978) has identified cultural variables like language translatability, language structures, color perceptions and color categories, ecological perceptual styles, and field independence. It is supposed that the list of variables can be used as a basis for developing Web sites that locally adapt the spatial orientation of Web privacy practices. In the privacy process, the cultural sensitivity of Web sites can be developed in terms of country-specific symbols, icons, and color symbolism (for example red for vulnerability items and green for protective items).

4.7.5 Possibilities of Modularity

Although the advance of modular design typically concerns a complex multi-level organization (Earl and Kay, 1985), it seems that the modularity category scheme entails progress to appropriately consider the privacy situation in the organization from the perspective of actions. Activities at different levels in the organization typically have different tasks, actions, and goals and the privacy practices vary accordingly. Even if the Internet company is a single-level organization, the informationally-enriched processes and the use of technology may alter a lot as we move between activities. It is neither the kind of data nor the content of the data itself that will determine the privacy matter. Instead, it is the situation in which the knowledge is used that we must consider. Therefore, a privacy process using the layered privacy model and different categories seems to provide advantages for every organization.

First of all, it is possible to consider each category of modularity structure individually. The importance of each modular category revision may vary between activities. It is possible that some privacy process steps of the category are not necessary in every level of organization. In addition,

modularity category schemes provide the opportunity to accomplish the privacy process using different tactics than those presented in Table 15. Some modular category revisions need to be done often and some are long-term by nature.

Secondly, the modularity category scheme provides a good basis to revise privacy practice using several specialists. It offers the chance to use professional knowledge (e.g. risk-based analyses by a technical specialist or assessment by a jurist for legal issues), but also local special (e.g. tacit) knowledge to implement and evaluate privacy practices. This kind of approach has the potential to reveal employees' interest (motives, incentives, and purposes) and perhaps refinement of employees' values are needed.

Thirdly, the privacy manager is able to make useful checklists using the modularity category scheme. Those checklists help with the scope of the privacy process. They may also form standard operating privacy practices. The process of writing an effective privacy policy can be guided by ensuring that all modularity categories have been considered. The activities of the checklist are not described in terms of information technology but in terms of the organization's activities and actions. It gives privacy managers a wider understanding of the privacy situation. It also provides a means to guide communication between specialists and employees as they evaluate and form privacy practices for the organization. Prepared checklists are a step in the direction of clarity and accuracy, but also in the direction of preventing some misunderstandings and failures in advance. For those reasons, the legal category is strongly entitled to be one category of special knowledge. Additionally, the health care business, including HIPAA and other special law issues, point out the importance of the legal category. Legislation-based checklists are not limited in their application to privacy concerns involving technical artifacts. They are able to cover a much wider area of privacy issues, including those health processes and practices that are not computer-supported.

Judith Donath, an MIT professor who studies identity and online behavior, says that until Web sites design spaces that are clearly public or clearly private, users will have trouble choosing what to share and what to hide. She adds that such fundamental decisions about what to share "*shouldn't be about reading the fine print*" of a Web site's privacy policy, but instead should be as obvious as the difference between staying in the privacy of your own home versus walking down the street. When the user is in "*private*" space, he would have the right to expect that nothing about his activities there would be monitored, gathered into a profile, or sold to anyone or any firm unless he

authorizd it. Just as people act one way in their dens and another way at a party, Internet users want to make sure that the Internet world recognizes nuances about when "*public*" and viewable events are occurring as opposed to "*private*" and sensitive communications (Fox, Rainie, Horrigan, Lenhart, Spooner, and Carter, 2000, p. 10).

And fourthly, the modularity category scheme and the balanced privacy model offer a means and advantages for more customer-friendly privacy policy design. Based on the media richness theory, it is suggested (El Sawy, Eriksson, Raven and Carlsson, 1999) that richer media should be used to a larger extent for collaborating and that less rich media should be used to a larger extent for informing. Considering the customer's needs presented in Table 15 and the media richness theory, it is possible to propose the following media forms and types in Table 16.

Table 16: Suitable Media for the Modularity Category.

Category	***Media Form***	***Media Type***
Legal	Seal	Informing
Business	Interactive	Collaborating / Informing
Contractual	Interactive	Collaborating / Informing
Social	Interactive	Collaborating
Technical	Seal	Informing

The media richness theory (Daft and Lengel, 1986) suggests that in situations and actions with high uncertainty, a suitable media should be rich. Seal is a lean media but it is a very suitable media for informing about the secure and strict normative principles of the Web site.

By focusing on electronic transactions, the privacy regulation required by HIPAA aimed to give consumers confidence that as the health information system moved to a networked, electronic, computer-based system, their most sensitive health information would be protected. However, the HIPAA rule only applies to a covered entity and protected health information, so it may create an illusion of legal protection that may lull consumers into a false sense of privacy when they engage in online health activities. Consumers may believe that the personal information they provide to health Web sites is protected by the new regulation when in fact many web sites will remain unregulated, as discussed earlier. Slater and Zimmerman (2003, p. 1282) also studied the Web portals that deliver health care Web sites to customers. Their listings of search results provided by the most widely used Web portals do not often provide basic information that a consumer would need to select an

objective and reliable health information Web site. Nowadays, health consumers must rely on a brief site listing generated by portal searchers when deciding which Web site to access. This list does not indicate any privacy issues. It is an important matter because previous studies pointed out that most customers just plunged right in to see what they could find rather than asking anyone for advice about which Web sites to use. In particular, those who used a search query engine were more focused on getting the information fast than finding a trusted name.

Effective metaphors can be used to express organizational privacy practices and bridge the gap between Web site privacy practices and consumer understanding, thereby increasing their clarity and visibility. Seals make it easier to recognize private and public situations by a customer. If a Web site honors normative privacy acts, for example HIPAA, then "*HIPAA seal"* would be very suitable metaphor to indicate that. A seal has the capability to give more basic information to customers in cases where different privacy regulation rules may apply to different Web sites offering the same services. That information can be included in brief site lists of the Web portals. At Web sites that are owned or operated by organizations covered by the privacy regulation, it is unclear which activities at those sites are subject to the privacy rule of HIPAA. In those cases, the HIPAA seal seems to be useful when the indication happens per activity. This practice indicates when a customer is covered by the privacy rule (i.e. in privacy space) and when a customer is not covered by the privacy rule (i.e. in public space). Technical security issues can be directed in the same way. If the Web site protects customer security through 'engineered' means, for example messages are securely encrypted using the most advanced techniques, then customers can expect a high level of security. A seal indicating the secure technical matter seems to be very practical media. A seal on the Web site and on the site list of the Web portals means that the matter becomes more visualized and it may support the visibility category scheme. It is an important advantage for the users to understand what they are agreeing to and this in turn invites a high level of trust within the organization as well as perceived trustworthiness from those outside the organization.

Those kinds of practices can be used to deal with seals when flexibility is not needed. Considering the balanced privacy model, the seal does not provide enough flexibility to support the Privacy-on-Demand and Service-on-Demand functions sufficiently. A seal seems not to be the best practice for categories where flexibility and collaborating options are needed. Privacy seals have the potential to provide assurance for some but not all privacy and security

matters, as discussed in Section 4.4. The functions of Service-on-Demand and Privacy-on-Demand require richer media for clarification and verbal discussion, at least in the health care context[97].

While we are waiting for more sophisticated applications, online companies are already able to "easily" express their privacy practices more understandably and in a manner designed to call attention to the nature and significance of the privacy situation using the modular structure of category-based privacy policy. For example, if all contractual-related privacy practices were expressed in the contractual section of the privacy policy, it would be beneficial for customers who want to know about the protective and vulnerability items of the contractual matter. The date of the latest revision of contractual-related privacy practices should be clearly posted on the homepage of the Web site. The revision dates of each modularity category displayed on the homepage of the Web site do more to describe the type of change that occurred. The contractual section of the privacy policy may include all possible contractual options to opt-in and opt-out. This privacy management enables customers to choose preferences concerning contractual matters using the interactivity properties of the Internet. Other modularity category items can be expressed similarly in their own section of the privacy policy. It is important that a privacy policy be available to users without requiring extensive searching and reading processes, and the modular structure of the privacy policy provides some remedy for this.

4.7.6 Motivations for Privacy Process

The term privacy manager is used in this study. The basic reason is underline that appointing a privacy manager is one way of galvanizing, directing, and coordinating the privacy process or campaign. It is not likely to be sufficient alone; nor is it likely to be universally necessary. But under the privacy rule of the HIPAA[98], a covered entity will be required to designate a privacy manager to develop and implement the entity's policies and procedures; train its employees; implement administrative, technical and physical safeguards; develop a method for handling complaints; and develop sanctions for members

[97] More technical oriented innovations, for example the Privacy Preferences Project (P3P, http://www.w3.org/P3P) and Privacy Bird (http://www.privacybird.com), are good in many cases but in order to pursue the balanced privacy model they have the same weakness.

[98] Privacy rule, § 164.530(a), available at http://www.hhs.gov/ocr/regtext.html

of its workforce who fail to comply with its privacy policies or procedures or with the requirements of the rule. The regulation imposes such requirements to ensure that appropriate members of the covered entity are familiar with and comply with the privacy rule, and that covered entities will be held accountable for the actions of their employees.

It is likely that many organizations have invested in aspects of privacy without appointing a privacy manager. However, today's privacy managers are discovering that privacy management comprises a large agenda and that making substantial progress takes time. Thus, a privacy manager or coordinator can keep up the momentum and distill, codify, and share learning about organization's privacy capabilities and practices. In every reasonably complex human activity, decisions are made which require value choices at least implicitly. Business people make value decisions about good investments, lawyers make decisions about good jurors, and privacy managers make value decisions about good privacy practices. All of these endeavors utilize facts, but the facts are always accompanied by values (Moor, 1997; Moor, 1998). Each discipline has its own cluster of values that members of the discipline use in making decisions. Therefore, appointing a privacy manager may be a good place to start when embarking on a privacy process, even if the online company is not a covered entity. The empirical part of the study points out that privacy managers have much work to do and the challenges are huge. Privacy managers need a privacy process for more secure systems, more enforceable privacy policies, increased transparency, and more choice for consumers in the spirit of the balanced privacy model. There are many different categories and principles to consider, so finding the right person is at least as important as deciding to create the role.

Based on this study, it is possible to conclude that the development of privacy practices is a very quality-dependent issue. There are so many principles, properties and situations to consider. There are different kinds of activities within or without information technology and each plays its part in the total arc of work, either separately or collaboratively. There is a lot of informationally-enriched standard operating procedures, articulation work, and situated actions in the health process. Considering Leavitt's Diamond, situated actions without plans, and the unpredictable nature of articulation work, these sequences of activities include many potential privacy threats. Since more people are involved in the health process, each person may be involved with sensitive information. One weak link in the series of privacy practices can cause online organizations to become vulnerable to legal challenges, dissatisfied customers, and/or strained relationships with other organizations.

Therefore, rather like total quality management, privacy management should become embedded in organizations and trust should become an obviously imperative source of value creation and competitiveness. The qualifications for successful privacy management depend a lot on the motivation for activities, especially in the knowledge-sensitive business segment, where the vulnerability of customers may be very high. Psychologists and sociologists more generally distinguish between two kinds of motivation, extrinsic and intrinsic (Kreps, 1997). Extrinsic motivation is induced by manipulations of rewards or sanctions from the outside, and intrinsic motivation occurs when people perform an activity for its own sake because of reasons lying within their own person (Frey, 2001, p. 14). Anybody looking at successful privacy management must be aware that a phenomenon such as intrinsic motivation does exist. Extrinsic rules and incentives may destroy the workers' intrinsic motivation, leading to a lessened level of quality-weighted effort (Kreps, 1997). Effective privacy management demands that all members of the organization will own and drive privacy management. Privacy management is a very sensitive business, and therefore intrinsic motivation should receive special focus to also bring up tacit knowledge and hidden practices (Nonaka, 1994).

4.7.7 Conclusion

Based on the analyses of privacy policies, the privacy process should be aimed at a much wider focus than only IT-supported activities, which is one message of the layered privacy model and modularity category scheme. The Internet revolution now engulfs the whole company, and it is crucial that the issues of privacy be addressed on every level of the organization. It is important to gain wide knowledge of the privacy situation, including an accurate and exact view of specifications. The privacy process indicates the importance of privacy issues to be considered holistically, where one weak link can mean vulnerability to customers and organizations. Privacy managers should maintain a holistic view of privacy in their organizations in tandem with how the presented categories (major, visibility, and modularity) constrain and influence information practices. Only by close analysis of organization can a privacy manager effectively design and manage the privacy issues of an organization. In a privacy process, the whole organizational context and several business processes should be taken into account.

The Internet is an effective tool for receiving and sharing data and, thus, the Internet has a range of capabilities that health providers are using to exchange information internally or to communicate externally with other organizations. Business functions on the Internet are, however, relatively new, resulting in modifications to how some organizations conduct business. Thus, along with bringing many new benefits and opportunities, the Internet has created a new set of management challenges. Change in organizational objectives, business protocols, organizational focus, and management are some reasons why the practices and policies of an organization might change. The extent to which the subject matter appears unpredictable and vulnerable will vary according to the level of the service functions and the sensitivity of customer information. The privacy process should focus openly on privacy issues through the different lenses of modularity categories at every relevant level using different tactics. The priorities also come from such understanding, thus determining what to do first.

The privacy process offers the criteria for modifying privacy practices and policies and designing new ones to balance customers' interest in privacy with the benefits of having so much information, and to balance the rights of customers to privacy against the desire of companies to use this technology to improve their marketing and to better target their products to the interests of customers. All steps of privacy process help form a consensus about acceptable privacy policies, but some residue of disagreement may remain. However, a residue of ethical difference is not something to be feared. Disputes occur in every human endeavor and still progress is made. Privacy management is no different in this regard. The chief threat to the privacy process is not the possibility that a residue of disagreements about which privacy practices are best will remain after debates on the issues are completed, but a failure to debate the ethical issues of privacy aspects at all.

An important aspect of the balanced privacy model is that normative privacy is contingent on certain situations or zones, and thus cannot be grounded simply in terms of the information itself. Some tasks can be predicted and privacy practices made for them. Yet each actor, individually and collectively, has a domain of responsibility that is exposed by unexpected situations (articulation work and situated action). People have to then cope without expressed privacy practices. They have to rely on their understanding of the privacy situation and its objectives, and therefore the combination of intrinsic motives and extrinsic incentives can be one solution to reaching a high level of the balanced privacy model. Thus, companies have good chances to offer Internet services widely with trust.

5 SUMMARY

5.1 Background and Study Questions

The role of the researcher in this dissertation should be seen as a rationalistic knowledge builder inquiring about privacy practices from the perspective of an online customer and focusing on a more communicable and usable understanding of privacy practices. More research is needed to address how we as a society use, value, and protect citizens' personal information because privacy is a broad and, in many ways, elusive concept. Privacy is, however, grounded instrumentally and intrinsically – instrumentally, in support of the core values, and intrinsically, as an expression of security and more. In a computerized culture, the concern for privacy is legitimate. There is a presumption throughout this study that privacy is a positive value that is worth protecting, and that the federal health privacy regulation does not provide adequate support for that.

In the academic literature and the business press, there seems to be a lack of guidance and a lack of privacy policy assessments to support companies on the Web. This dissertation provides greater understanding of the definitions of and basis for privacy protection on the Internet. This dissertation presents the criteria for modifying privacy practices and policies and designing new ones to balance the rights of customers to privacy against the desire of companies to use this technology to improve their marketing and to better target their products to the interests of customers. This understanding is critical because consumers are becoming increasingly privacy aware and more interested in knowing how to protect their own privacy. At the same time, health care companies are increasingly transferring their informationally-enriched health processes onto the Internet for new business practices.

The focus of this study is on the information-rich business segment of the health care service where the user vulnerability is exceptionally high due to the sensitive nature of information collected at these Internet services. The protection of customers' personal health information is not an option but a necessity. The Internet has become a major catalyst for both electronic commerce and electronic business, and it is being taken into usage in the health care segment at in increasing pace. The Internet is an effective tool for receiving and sharing data. Since more people are involved in the health process, each person may be involved in sensitive information. Health care

privacy, as it pertains to organizational practices, holds profound implications as service delivery impacts on human life, legality, and social policy (Darr, 1997). Any organization embarking upon online health care transactions should be prepared to address privacy matters and adjust its policy accordingly.

Efficiency is one of the reasons why people like to use the Internet, and privacy and security issues are cited as the top reasons why more people do not use services online or complete the transactions they start. Sharing personal medical and health information across the Internet requires a certain leap of faith – or at least a strong sense of privacy and trust. Consumer privacy concerns can pose a serious impediment to the expanded growth of electronic commerce and Internet usage. Because of uncertainty and unpredictability, Internet services may function ineffectively and it is possible that the potential of new Internet services might be only partially used.

In a virtual world the issue of trust gets magnified, because trust is a critical factor in any relationship in which the consumer does not have direct control over the actions of online company, the decision is important, and the environment is uncertain. Medical information is increasingly protected. Expectations for its privacy are therefore increasing reasonably, but one key detail of the Internet is that there is no such thing as “absolute privacy”. The rapid advance of the Internet has mounted serious challenges to customers’ intuitive sense of privacy. Customers provide a great deal of personal information and sensitive health information in the course of obtaining health care, yet there is little legal protection for health information – online or offline. Customers worry that their health information may be used or disclosed inappropriately. As a result, consumers sometimes take drastic steps to keep their health information private.

The United States was chosen because there electronic commerce is being taken into usage in the health care segment at an increasing pace, and the legal issues of privacy matters are mostly on a voluntary basis. The mechanism by which consumers are typically made aware of a U.S. company’s privacy practice is through the presence of a privacy policy. Privacy policy statements interact to produce and sustain an online presentation of the company and produce a convincing performance. Privacy policies inform consumers about how organizations collect and use their customer information and theoretically serve as the basis for consumer browsing and transaction decisions. The finding of Choy, Hudson, Pritts and Goldman study (2001, p. 4) is that a significant portion of activities at health-related Web sites are not covered by U.S. privacy regulations (HIPAA), and therefore, a Web site privacy policy is

an important document to reflect the practices of the online health organization.

This study seeks to understand how expressions given and given off in 39 U.S. health care privacy policies are adapted and managed in an online context. The privacy policies were analyzed to develop an understanding of the current state of e-Health privacy practices. This explorative study discovers, names, and categorizes privacy policy items and develops categories in terms of their properties. Beyond simply cataloguing expressions, the study interprets the quantitative findings to comprehend how these expressions interact and shape the presentation online.

The research questions that guide this study are:

- What are the requirements for a good privacy policy of a Web site?
- What communication practices of privacy matters are found in health care Web sites?
- What are the typical contents of a health care Web site privacy policy?
- How to assess the content and communication of privacy policy?

To answer these questions, a content analysis of expressed online privacy policies was conducted. The aim of this study is to provide information about the nature of privacy as it is perceived in electronic commerce, and privacy policies are a reflection of that usage. Privacy policies are public organizational records, which are considered to be a form of interaction among customers, organizational constituents and, to a lesser extent, between the constituents of competing organizations. Privacy policies are valid gauges for content analysis because they capture how organizations express significant values, emergent issues, and ongoing activities and practices to customers. The study context within voluntariness and high sensitiveness makes the assessment of privacy issues more challenging.

Issues concerning users' privacy protection on the Internet have been studied, and in particular, discussed extensively for some time. Several researchers have provided various approaches to creating sufficient data protection for consumers. A lot of emphasis is placed on data protection and confidentiality issues to prevent unauthorized use. Many of these approaches outline technical measures for providing better security, which in turn provide a higher potential for data privacy. Reducing threats to sensitive data is also the focus of several studies addressing technical methods to provide better security for data privacy. Organizational routines and norms direct employees' actions, resulting in cumulative privacy policy utilization to support organizational goals, but by doing that they may also constitute a privacy threat to customers. Some researchers (Smith, Milberg and Burke, 1996) have

realized the need for validated instruments for measuring individuals' concerns about organizational practices. Their idea is that because employees of any organization are ultimately in control of sensitive customer information, it is important to understand employee attitudes, as well as consumer attitudes, toward privacy. Understanding the attitudes of employees, who have regular access to personal information, will assist the field in developing better methods for privacy protection.

All those previous studies are vital for effective data protection, but they are not wide enough or they lack a much-needed mechanism to evaluate the privacy element in more detail in the context of e-Health. Though many studies have examined the information available on the Internet, both in terms of the customer's experiences and the quality of the information, little work has been done to evaluate the privacy practices of the Internet for health-related activities. The revolution in health care information has great potential to affect the way in which customers' privacy is understood, but relatively few have studied expressed online privacy policies in the health care business segment. Previously privacy policies are evaluated in a rather ad hoc and inconsistent manner, but there is, at least, one exception. The study by Goldman, Hudson, Smith (2000) focused on the policies and practices of 21 health-related Web sites. The Web sites were selected to represent a mix of the most trafficked consumer health sites in the following groups: Web sites where consumer desire for anonymity might be more precious, Web sites where pharmaceuticals and health products may be researched and purchased, general search engines or portals that get a high degree of Internet traffic, and Web sites that target a specific demographic. They reviewed the privacy policies of each Web site and investigated whether their actual practices reflected their stated policies. Their method of investigation was to review the stated privacy policies against a set of "*fair information practice principles*" and to behave like a typical consumer on each Web site and observe and capture what happened to the data that was submitted.

Our challenge is to take full advantage of the Internet without allowing the Internet companies to take complete advantage of us, and therefore thoughtful analyses of newer privacy situations in which the Internet has an impact are needed. This thesis studies the privacy policies of health care Web sites to get more practical and useful knowledge of the privacy practices of electronic commerce and, more specifically, the identification of different categories for further use. The older studies do not give sufficient concept to answer questions like how to balance customers' interest in privacy with the benefits of having so much more data? And how would it be possible to balance the

rights of customers to privacy against the desire of companies to use this technology to improve their marketing and to better target their products to the interests of customers? In addition, there is no agreement on how we should do the revision and evaluation of privacy practices and policies, and which kind of factors ought to be taken into account. The most published work relating specifically to health Web sites has focused on descriptions of individual Web sites rather than on assessments of the whole and the separate business segments. This research was undertaken to provide an overview of Web site privacy issues within the health care industry as a whole but also to provide an overview of the privacy aspects and issues found in five health care business segments: pharmaceuticals, health insurance, online drugstores, medical institutes, and general health information. For those reasons, a wide combination of qualitative and quantitative methods has been used in this study. This study seeks to increase the understanding of privacy policy as a significant trust indicator for fair business practices. The objective of this study is to develop instruments and categories to assess the content and communication of privacy policy. Rational approaches can be used to deal with evaluation of privacy policy, and therefore the main features and involved categories for privacy policy metrics are delivered. Discovery is the primary focus of this explorative study and data collection; the analyses and the associated theoretical sampling are structured to allow for this.

5.2 Research Process

In order to identify the used communication practices of privacy matters in health care Web sites and to identify the typical contents of health care Web site privacy policies, a content analysis was employed to derive the privacy-related items of 39 U.S. Internet Web sites. During the study, process privacy policies were broken down into discrete items from the following health care privacy policies: six pharmaceuticals companies, seven health insurance companies, ten online drugstores, six medical institutes/disease-specific Web sites and ten general health information Web sites.

To answer to the study questions, it was important to uncover all significant, important, and interest items, along with the most relevant categories and their properties. Item identification and item reduction were the core part of the analysis that pertained specifically to the naming and categorizing of privacy matters through close examination of privacy policy statements and the theoretical frameworks. It was crucial to maintain a balance

between consistency (that is, systematically gathering relevant data about categories) and the making of discoveries (uncovering new categories). An investigation of the way in which the "*privacy*" is understood using theoretical privacy frameworks (the core value framework of privacy, the balanced privacy framework, and the balanced privacy model) would provide a "*reality check*" on the conceptual development. To systematize and solidify connections, a combination of inductive and deductive thinking is used, which constantly moves between asking questions, generating propositions, and making comparisons. For this study every effort was made to ensure that each of the 39 privacy policies in the sample was evaluated using the same categories, coding schemes, and same theoretical knowledge.

Content analysis was used in the privacy policy study, because content analysis is regarded as an appropriate technique for analyzing values and norms of behavior. The author used it systematically to assess the content and communication of an online health provider's privacy policies, and the findings reported here confirmed that it could be used in this kind of study successfully. Content analysis allowed privacy policies to be analyzed in a transparent and reproducible manner. Secondary sources provided unobtrusive access when examining sensitive situations, and eliminated distortion due to imperfect recall and social desirability bias. The use of content analysis for studying privacy policies brought additional benefits to the overall research activity. It allowed an assessment of the validity and reliability of the empirical research to be made, and meant that the categorization process and the basis for categorization were clearly specified and open to scrutiny. There are, however, some limitations to secondary data when setting e-commerce privacy practices. The used technique does not reveal those privacy matters that are not expressed in privacy policy statements, for example, it does not reveal the number of security and privacy incidents in the company.

5.2.1 Theoretical Background

Robertson (1993) and Randall and Gibson (1990) point out that many studies set out to measure abstract variables without providing a theoretical foundation upon which to base the definition or the constructs. However, theoretical sensitivity represents an important creative aspect of this study. Theoretical sensitivity is the ability to recognize what is important in the data and to give it meaning. This sensitivity represents the ability to use not only personal and professional experience imaginatively, but also literature.

Theoretical sensitivity enabled the analyst to see the privacy situation and privacy policies in new ways, and to explore the data's potential for identifying and developing but also reducing items accordingly. To determine whether the privacy practice or policy of a Web site actually violates the privacy of customers, it is important to describe useful privacy frameworks as precisely as possible. Such frameworks should enable us to differentiate "*good privacy policies and practices*" from "*bad ones*".

This study included a wide set of efforts that were performed to increase theoretical sensitivity. In order to identify the demands for a good privacy policy of a Web site, the author presented three privacy frameworks based on theoretical knowledge: the core value framework of privacy, the balanced privacy framework, and the balanced privacy model.

First, a theoretical core value framework of privacy was presented, i.e. privacy is a positive value that is worth protecting. When the ethical problems involving the Internet are considered, none is more paradigmatic than the issue of informational privacy. Given the ability of information technology to gather widely, to store endlessly, to transfer cheaply, to sort efficiently, and to locate effortlessly information, we are justifiably concerned that our privacy may be invaded in the Internet world and that information harmful to us may be revealed. Privacy is becoming a standard issue for Internet ethics, because the widespread use of Internet services and the complexity of the Internet infrastructure is a combination that makes solitude and privacy more essential to the individual. The core values were emphasized because they provide a set of standards by which it becomes possible to assess the activities of different people and different cultures. This global entity of core values provides us with reasons to prefer some privacy policies and practices on the Internet over others. However, the framework has room for individual and cultural variation as proposed by the balanced privacy framework and the balanced privacy model.

Second, the author determined the balanced privacy framework. It was drawn on the core value framework of privacy, the control and restricted access theory combined with the publicity, the justification of exceptions, the adjustment (Moor, 1997, 1998; Tavani, 1999a, 1999b; DeCew, 1997), the mischance, the positive voluntary, and the negative voluntary principles (McArthur, 2001). This study explores the concept of informational privacy, and information practices may conflict with consumers' desires to be shielded from unauthorized use of their personal information. The balanced privacy framework puts the focus on what we should be considering when developing policies for protecting our privacy in that situation. It does not neglect the

important distinction between the different interests affected by electronic commerce. The balanced privacy framework gives individuals as much control (informed consent) over personal data as realistically possible in a certain situation. The balanced privacy framework helps us to determine whether certain kinds of personal data should be considered private or public data in a privacy situation. The balanced privacy provides a procedure for determining whether the privacy policy statement is vulnerable or not in a privacy situation.

Third, the author determined the balanced privacy model. It was drawn on the balanced privacy framework, the trusted balance – scenario (Pearson, 2003) and exchange theory (Thibaut and Kelley, 1959). According to exchange theory, individuals form associations on the basis of trust, and try to avoid exchange relationships that are likely to bring more pain than pleasure. In the balanced privacy model, customer privacy (Privacy-on-Demand function) is related to the function of service (Service-on-Demand function). Employing an interactive dialog by demanding or consenting, customers are able to choose from "*rich service*" to "*lean service*" to be polarized into the concept of privacy, i.e. "*publicity*" or "*secrecy*". The interactivity features of the Internet have the means to make privacy issues more exact to consumers, thus enabling them to choose privacy practices and make more informed decisions concerning to whom they entrust their personally identifiable information and what kind of service functions they prefer and or don't prefer. If a company changes the privacy practice without consent or demand by the customer, it may be leaning toward opportunism or deficit electronic commerce business.

The interactivity features of the Internet give online companies many possibilities to manage so that the customers can make the most convenient choices considering their own needs and values. What one user considers a privacy invasion may be a valued feature or service to another user. Interactivity is a pivotal and much debated concept used to evaluate the overall quality and responsiveness of the Internet. Interactive Web site content can provide considerable added value for both the company and its customer. In this study, interactivity has been understood as the degree to which the customer is able to choose and *"manipulate"* service and privacy practices. High interactivity means more conscious and open data process; more choices; and more predictable consequences. Interactivity combines elements of connectedness to the audience, use of natural language, ability for information sharing and informed consent, and reciprocity.

5.2.2 Categories

Content analysis is the analytic process by which items are identified and developed in terms of their properties. The basic analytic procedures by which this is accomplished are the asking of questions about the data; and comparisons to find similarities and differences between each item and other instances of phenomena. Once items are identified, they are elaborated. Item elaboration entails analyzing each item for the purpose of documenting item properties. After a deduction the items are grouped together under a higher order. Questions like, "*What is this?"* and "*What does it represent?*" are asked. Once particular phenomenon is identified in the data, it is possible to begin to group items around them and through the coding procedures they earn the status of categories.

This study led to the development of privacy item categories and enabled codification of a comprehensive set of coding schemes tailored to the content analysis of privacy policies. It is important to think about privacy policies analytically rather than descriptively, to generate provisional categories and their properties, and to think about generative questions. It is also important to recognize and systematically develop properties because they form the basis for making relationships between the major categories, categories, and subcategories. The categories into which the items are to be placed must be grounded in the data from which they emerge and from the theoretical knowledge that the analyst brings to the task. Three privacy frameworks, the major category scheme (i.e. protective and vulnerability), the visibility category scheme (i.e. visible and invisible category), and the modularity category scheme (i.e. legal, business, contractual, social, and technical category) have a central role in that process.

Privacy policy taxonomy was created by Antón, Earp, and Reese (2002) in the first phase of the privacy policy study. It aimed at identifying privacy policy goals that reflect or contribute to protective or vulnerability matters. Privacy policies should express the ways in which they protect personal information but, according to the Fair Information Practice Principles, Internet companies should also inform their customers of potential vulnerabilities that may threaten one's privacy. According to the taxonomy, privacy protective goals relate to the desired protection of user privacy rights, whereas privacy vulnerability goals relate to existing threats to consumer privacy. The initial empirical studies were done based upon the use of the Goal-Based

requirements Analysis Method – GBRAM (Anton, 1997; Anton and Potts, 1998)[99]. The author used content analysis in this dissertation. Protective and vulnerability taxonomies are called major categories because other (sub-) categories used in this study can be subsumed under them as properties and strategies. In addition, the author has further developed the basic protective and vulnerability taxonomy concept, adding theoretical sensitivity for consideration. The core value framework of privacy, the balanced privacy framework, and the balanced privacy model enable the analyst to see the privacy situation and privacy policies in new ways, and thus, to explore in more detail the data's potential for identifying and developing but also reducing major category items.

Protective items are categorized by analyzing each item and asking the basic question[100], *"Does this item potentially foster the privacy and/or security of one's privacy situation?"* Theoretical sensitivity gives us more theoretically-based evaluation criteria to make decisions, and therefore it is important to consider, *"Does this item support the core value framework of privacy?"* and/or *"Does this item support the balanced privacy framework?"* and/or *"Does this item support the balanced privacy model?"* The additional questions give us more theoretical arguments for assessment.

In contrast to protective items, vulnerability items are those related to existing threats to user privacy. They represent statements of fact or existing behavior, and are often characterized by privacy invasions.

Vulnerability items are categorized by considering each item and asking the basic question[101] "*Does this item potentially compromise the privacy and/or security of one's privacy situation?"* and the more theoretical consideration, "*Does this item conflict with the core value framework of privacy?"* and/or *"Does this item conflict with the balanced privacy framework?"* and/or *"Does this item conflict with the balanced privacy model?"* gives us more convincing arguments for assessment.

Some interpretative problems of categorizing may evolve. Some privacy invasions are benign or can at least be interpreted by some customers that way.

---

[99] The GBRAM is a methodical approach to identify system and enterprise strategic and tactical goals as well as requirements. Goals are the objectives and targets of achievement for a system. The method suggests goal identification and refinement strategies and techniques through the inclusion of a set of heuristics, guidelines and recurring question types.

[100] The author has modified the GBRAM-type question originally presented by Antón, Earp, and Reese (2002), converting it into content analysis format. The author has also added the consideration of three privacy frameworks to see the privacy situation in more detail in order to further explore the data's potential for identifying and developing but also reducing items accordingly.

[101] The author has changed the original vulnerability concept accordingly.

The problem is what one customer considers a privacy invasion (vulnerability items) may be a valued feature or service to another customer. From the customers' perspective, it is important to help customers evaluate and make decisions between practices that protect their privacy and practices that may introduce potential vulnerabilities, and the core value framework of privacy provides a set of privacy standards by which we can evaluate different privacy policies. The balanced privacy framework and the balanced privacy model also provide more exact criteria to evaluate each item accordingly. Interpretive problems can be managed by carefully considering each item's actual intent. The balanced privacy framework and the balanced privacy model tell us what to look for when making our assessments about the benefits and harms of different privacy policies and practices. They give us the reasons for preferring one privacy policy statement over another.

The visibility categorization scheme expresses two categories that must be considered when evaluating an organization's privacy policy, specifying system requirements, and designing Internet software. The categorization scheme reflects the visible and hidden natures of privacy management practices, which are studied within the context of privacy protection and vulnerability (Jarvinen, Earp, Antón, 2002).

Visible privacy practices are performed in such a way that an average Internet user is aware of data collection while accessing Web sites with a browser using default security and privacy settings. The items that are easily observed and evaluated by the user are calculated as visible items. The visible process typically occurs when a user fills out a form, sends emails, or responds to a survey. All of these circumstances require the user to actively and consciously decide whether or not to provide the requested information. It is considered to be a conscious process when the user knows they are voluntarily disclosing information and is able to prevent the disclosure if so desired.

Invisible privacy practices are performed in a hidden manner that requires users to take a proactive role in learning about Web site privacy practices (e.g. reading the privacy policy, setting the browser's security and privacy settings, learning about cookies, etc.) The concern for privacy is justified because whenever an Internet customer visits a Web site, a large amount of customer information may easily become available to the Web site owner. The majority of data exchange between a customer and an Internet service is visible to the customer, but there are many methods in which the Web site can gather information without the customer being aware of this, including cookies and data mining.

Visible and protective items are categorized by analyzing each item and asking, "*Does this item support the core value framework of privacy and is it apparent to the user without reading the privacy policy statements?*" Visible and vulnerability items are categorized by asking: "*Does this item conflict with the core value framework of privacy and is it apparent to the user without reading the privacy policy statement?"* Invisible and protective items are categorized by asking: "*Does this item support the core value framework of privacy but is it not apparent to the user without reading the privacy policy statement?*" Invisible and vulnerability items are categorized by asking: "*Does this item conflict with the core value framework of privacy and is it not apparent without reading the privacy policy statement?"*

It is possible to consider how those sub-categories support the balanced privacy framework and the balanced privacy model. The categorization scheme is proposed to aid in the design of Web sites to focus on visibility and protection, but also visibility and vulnerability. Those two sub-categories reflect practices of the balanced privacy model, whether protective or vulnerability, in that they are immediately visible to the consumer. Invisible privacy management does not typically support the balanced privacy model sufficiently.

Some proposals and suggestions regarding how to deal with privacy issues involving information technology fall into one of two types of categories: proposals that are technology-based and those that are legislation-based. One advantage of legislation-based proposals over those that are technology-based is that legislation-based proposals are not limited in their application to privacy concerns involving technical artifacts. They are able to cover a much wider area of privacy issues, including those health processes and practices that are not computer-supported. On the other hand, legislation-based proposals do not appear to provide customers who might wish to opt-in to special features with a mechanism to do so.

It is apparent that a more structured framework is needed to adequately consider privacy issues within a broader and more sensitive organizational context. So while privacy enhancing technologies and legislation-based proposals provide a basic "*solution*" to privacy issues involving the use of personal information on the Internet, they both have weaknesses which need to be addressed. It is proposed that privacy management should be evaluated from several modular categories within an organization; these categories primarily include legal constraints, technical measures, business rules, social norms, and contractual norms (Earp, Antón, Jarvinen, 2002).

The *legal category* concerns legislation that must be adhered to and which constrains the other four categories. Legislative approaches center on how governmental agencies can best write public policy to protect privacy. The legal category, in a sense, constrains the business rules, technical measures, social norms, and contractual norms of an organization. The *business category* reflects the fact that business objectives and practices often pass through legal (and in some cases also technical) filters. Business objectives and practices center upon how data is collected and transformed into information that ultimately becomes a valuable business asset. The business category involved in e-Health has items that are motivated by social and contractual norms that further restrict the organization. The *contractual category* focuses on the binding agreements that form the basis for information exchange between an organization and its third parties or business associates. The contractual category focuses on how information transfer and information use by external organizations affects consumer privacy. The relationship between organizations and how they cooperate is looked at. If a user has the opportunity to make a choice about how his information is used, then the item is indicated as a social category item. The framework's *social category* focuses on organizations and their users (or customers) in terms of how customers and companies interact and cooperate to exchange goods, services, and/or information. The *technical category* offers tools and techniques that support and restrict the manipulation of consumer data. The technical category includes tools to support business objectives as well as social and contractual expectations; however, the limitations of technical measures may in turn constrain these objectives and expectations.

Legal items are categorized by analyzing each item and asking, "*Does this item have any legal implications?"* Business items are categorized by asking: "*Does this item directly support the organization's business objectives?*" Contractual items are categorized by asking: *"Does this item focus on the relationship between a given organization and its business partners (e.g. third parties or business associates)?"* Social items are categorized by asking: "*Does this item address the relationship between a given organization and its customers?"* Technical items are categorized by asking: *"Does this item focus on domain-specific implementation details?"*

The modular category scheme is submitted to provide a useful basis for analyzing and comparing the privacy situation within the context of privacy protection and vulnerability. The process of allocating (or classifying) major category policy items as well as visibility category items to each of the modularity categories refers to the capacity to view things in light of their true

relations or relative importance. The modularity category scheme seeks to aid the privacy manager in maintaining a holistic view of privacy within the context of their organizations in tandem with how those categories constrain and influence information practices.

The framework of categories offers a foundation for reasoning about privacy management from the viewpoints of the balanced privacy model. All categories play a key role in electronic commerce, especially when one considers that one weak link in the series of privacy practices can cause online organizations to become vulnerable to legal challenges, dissatisfied customers, and/or strained relationships with other organizations.

5.3 Summary of Findings

Every health care company in the sample did attempt to reassure potential customers by incorporating privacy policy statements into their Web site designs. It was anticipated that the health care privacy policies would contain matters on a wide variety of privacy issues, including management, legal issues, sensitive matters, politics, and community organizations, while also containing items of sufficient length for useful analysis. Both these assumptions were tested and confirmed in the pilot study.

The following presents the major findings of the content analysis:

- *Finding 1: The study points out that more protective item hits than vulnerability item hits are found in the analyzed health care privacy policies.*

The first finding gives a minor reason to consider high customer privacy. Privacy protective items relate to the desired protection of user privacy rights, whereas privacy vulnerability items relate to existing threats to consumer privacy, and therefore it seems that privacy practices are correctly covered. However, consumers are using health Web sites to manage their health better, but their personal health information may not be adequately protected.

- *Finding 2: The study points out that numerous examples of practices that make the customer vulnerable can be found in the analyzed health care privacy policies.*

Many practices suggest customer privacy is not a fundamental priority for those organizations. Most sites do not meet fair information practices – such as providing adequate privacy notice, giving users some control over their information, and holding business partners to the same privacy standards. Every analyzed health care Web site had a privacy policy, but several Web

sites required extensive searching to find either the revision date or to ensure that there was not a revision date available. Such a policy may introduce vulnerability to the user. In these cases, the responsibility is left to the customer to read and understand the entire privacy policy at every visit. If changes are unspecified, they are almost uncontrollable to the user. Basic site navigational tools like an internal search engine for privacy policies were not found on most of the health care Web sites. Additionally, many of the analyzed privacy policies contained technical and confusing language (i.e. unnatural language) that makes it difficult for the users to fully understand what they are agreeing to. The names of the company privacy managers and the provision of informational content such as the times when the privacy manager is available were noticeably lacking on all of the health care Web sites that were evaluated. This type of information would be helpful to prospective customers.

- *Finding 3: The study points out that the analyzed health care privacy policies contain obvious and visible privacy practices but also insidious and invisible privacy practice management.*

Visitors to health Web sites are not anonymous, even if they hope to be so. On a number of health Web sites, personally identifiable information was collected through the invisible privacy practice management. Through mechanisms such as cookies, data mining, keystrokes, mouse clicks, and click streams, health sites were collecting information about users, often without their consent. That is, information about which Web sites a user visits, how long he or she stays there, and where he or she goes afterward are recorded. This information is then used for future business decisions. Information such as the user's email addresses as well as the system and network characteristics of a user's computer was frequently recorded by Internet health companies. According to the study, invisible privacy management was more common than visible privacy management. In addition, the portion of the invisible and vulnerability sub-categories verifies that consumers are vulnerable to the insidious and invisible privacy practices of the organization. This finding means the user, who does not want to be misled by hidden tactics, has to read the privacy policy carefully.

- *Finding 4: The study points out that the privacy seal programs does not mean the reduction of uncertainty and risk for the Internet user.*

Half of the analyzed health Web sites has responded to the public's concern regarding privacy and security on the Internet through self-regulation by establishing privacy seal programs. Participating in a privacy seal program that already enjoys an excellent consumer reputation allows organizations to

distinguish themselves from the thousands of online services in a way that is easily recognizable by online users and that will instill trust and confidence in their health service. However, the privacy seal programs fall short of truly safeguarding consumers. An Internet Web site can display it regardless of whether or not a privacy policy truly protects user privacy. The study points out that the number of protective and vulnerability items in a health care privacy policy will depend on whether there is a privacy program seal or not on the Web site that posts that policy. However, the user lacks the ability to make an actuarial determination of the likelihood of privacy invasion – the privacy policy seal does not mean the reduction of uncertainty and risk for the health Web site user without the user first having to read the privacy policy statement. Privacy seal programs might have the potential to provide that assurance, but they do not necessarily mean full privacy protection and security.

- *Finding 5: The study points out that privacy policy content inevitably differs from Web site to Web site.*

If we compare the number of different category items between the analyzed privacy policies, we can conclude that in spite of the many guidelines and criterions, privacy policy content inevitably differs from Web site to Web site. It seems natural that Web sites that support rich business function require a privacy policy with many major and modularity category items. In contrast, Web sites whose primary mission is information dissemination with few transactions have little or no need to address so many privacy issues. The lack of terms and content standardization results in problems for those that want to compare different organizations' policies before deciding which organization to entrust their personal identifiable information with. During privacy policy formulation, the raison d'etre of the company lies in its ability to provide coordination. We must look at privacy policies as such media for communicating and collaborating information if we want understand their real function. This is a function that it fulfils less perfectly as the message grows less comprehensible.

- *Finding 6: The study points out that privacy management can be evaluated from several perspectives within an organization; these perspectives primarily include legal constraints, technical measures, business rules, social norms, and contractual norms.*

The legal category centers on how governmental agencies can best write public policy to protect privacy. It was expected that the legal items would provide privacy protection, but according to the study these were mostly privacy obstacles. The business category often centers upon how data is

collected and transformed into information that ultimately becomes business knowledge. The weight of business categorization was on protective, which reflects the business items as a positive trust indicator. The contractual category focuses on the relationship between organizations and how they cooperate. The majority of these contractual hits were categorized as privacy vulnerability items rather than privacy protective items. This implies that the organizations are not sufficiently aware of the vulnerabilities of their relationships with third parties. The social category reflects the direct relationship between the customers and the organization. Social items were primarily categorized as privacy protective items rather than privacy vulnerability items. This implies that the organizations are aware of the importance of their relationships with customers and try to support customer needs to protect privacy. The majority of those protective items also supported the balanced privacy model. The technical category takes into consideration how informational privacy is managed through 'engineered' means. Technology is used to protect users while also supporting the organizational goals of increasing and maximizing profits.

External validity and generalization describes the extent to which the study's findings can be generalized to other samples. The results reported here present evidence on the nature of the relationships between customers and health providers found in the privacy policies. The number of the studied Web sites and the scale reliabilities of the study measures give some evidence for generalization, but there are also many limitations to consider. In terms of making generalizations to a larger population, this study is not attempting to generalize as such but to provide aspects for consideration. This means that this explorative study applies to these situations and circumstances but no others.

5.4 Lessons for the Theoretical Background

This study involved the performance of a wide set of efforts to increase theoretical knowledge. By requiring the derivation of the categories, properties, and coding schemes from a theoretical sensitivity, the rigorous application of the eight-step content analysis procedure encouraged the author to develop closer links between the theoretical and empirical components of the privacy policy research, thus responding to the call from Robertson and others for a greater attention to theory. The inspiration for adding theoretical knowledge was to begin with the existing theory and attempt to uncover how

it applies to new and varied situations, as differentiated from those situations to which it was originally applied. The author presented two privacy frameworks mainly based on the older theoretical knowledge: the core value framework of privacy, and the balanced privacy framework. In addition, the author developed two more advanced business models for privacy management of e-commerce, the balanced privacy model and the layered privacy model. In the balanced privacy model, customer privacy (Privacy-on-Demand) was related on the function of service (Service-on-Demand), and it was drawn on the basis of theoretical knowledge and the reflections of analyzed privacy practices. The layered privacy model proposes a prominent strategy employed for coping with turbulent environments.

The management of organizational privacy practice should successfully anticipate many changes. Business functions on the Internet are relatively new, resulting in modifications to how some organizations conduct business. Change in organizational objectives, business protocols, organizational focus, and management are some reasons why the practices and policies of an organization might change. The Internet has created a new set of management challenges. The development of privacy practice in the turbulent environment of electronic commerce can be crystallized into one question: "*What ought to be covered and measured?*"

This thesis points out that the development of the Internet cannot be easily distinguished from the broader perspectives related to developing services as a whole, including ethical aspects. *We are entering a generation marked by globalization and ubiquitous computing. Therefore, the second generation of computer ethics must be an era of global information ethics. The stakes are much higher, and consequently considerations and applications of information ethics must be broader, more profound and above all effective in helping to realize a democratic and empowering technology rather than an enslaving or debilitating one.*

The contribution of the theoretical privacy frameworks is primarily intended to provide us with a set of standards with which to assess and develop privacy practices even in situations where no previous privacy policies or privacy regulations exist, and with which to assess other value frameworks when disagreements occur.

According to the core value framework of privacy, informational privacy is a positive and important value that is worth protecting. The core value concept provides a common value framework that makes it possible to assess the activities of different people and different cultures. This global entity of core values provides us with reasons to prefer some privacy policies and practices

on the Internet over others. The core values allow us to make transcultural judgments. When formulating privacy practices and policies, companies should try to minimize excess harm and risk to customers' personal information. It is an important matter of the Internet, because e-business will only grow if organizations and societies address privacy concerns. Even though there is a common framework of values, there is also room for much individual and cultural variation within the framework, as the balanced privacy framework, the balanced privacy model, and the layered privacy model propose.

According to the balanced privacy framework, the attempt to find one general measure for global privacy policy fails – there are too many situation-dependant aspects to consider. Privacy matters are deeply situation-dependent issues and cannot be found by applying a predefined list without considering the situation thoroughly. The strength of the balanced privacy framework is its ability to distinguish between the condition of privacy and the right to privacy and between a loss of privacy and a violation of privacy. It acknowledges the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings. In general, the amount of privacy customers have and can reasonably expect to have is a function of the practices and laws of society and publicity and voluntary principles. The rapid advance of the Internet has mounted serious challenges to customers' intuitive sense of privacy. Sorting through all of this is, obviously, a complicated matter, but the balanced privacy framework is a useful guide to reasonableness as customers struggle to ascertain how much privacy to expect. If privacy is understood not merely as a value involving the good of customers but as one that also contributes to the broader social and organizational good, then the concern for individual privacy might have a greater chance of receiving the kind of consideration it deserves.

According to the balanced privacy model, companies are competing to give customers the privacy they want. One important aspect of the balanced privacy model is that it proposes possibilities and advantages for customers and online companies. The balanced privacy model proposes flexibility for electronic commerce but also demanding rules and principles. The balanced privacy model normally illustrates the situation where a customer is able to give informed consent and to make rational decisions as the balanced privacy framework suggests – a customer is able to opt-in to (or opt-out of) privacy function and service function. In addition, the balanced privacy model has the potential to illustrate normative privacy practices, like law statutes. In that

case, the Privacy-on-Demand function has no flexibility in the privacy situation. An ideal case of normative privacy practice in a privacy situation, where everything is black or white, true or false, exists without any consideration of customers' values, Privacy-on-Demand, or Service-on-Demand functions. If we consider the core value framework of privacy, the balanced privacy framework, and the advantages and threats of electronic commerce in addition to the possibilities in the global setting, the balanced privacy model seems to be a suitable path to follow for electronic commerce.

According to the layered privacy model, a prominent and promising strategy employed for coping with turbulent environments is to devise methods of localizing and limiting the change posed by external demands, even if the source or form of the impulse cannot be clearly specified in advance. If individual privacy practice can be decoupled from the overall privacy policy without threatening the latter's integrity, then this may form the basis for privacy policy design in turbulent environments. In that setting, the author proposes an approach, the privacy process using the layered privacy model, to manage the privacy practices of an Internet company for dealing with unstable and unpredictable environments on the Internet. It is developed on the basis of the empirical privacy policy study, the framework of categories, and the privacy frameworks. The layered privacy model is submitted in order to agree on fair privacy policies, to enforce them, and to manage privacy issues in the spirit of the balanced privacy model targeted at building merited trust for electronic commerce. The privacy process proposes how the major, visibility and modularity categories can be used in constructive way within the layered privacy model in practice, and suggests ways to modify the policies to make them better. Recognition of many categories and organizational levels proposes techniques for the revision and evaluation of privacy policies in a setting where changes of technologies and development of services are pervasive.

5.5 Relevance and Contribution

This study is one of the first to address the relationship between consumer and business interests focusing on the Web sites privacy policies. A typical way to legitimate research is by explaining the value of it to the practice. Comparing privacy policies using numbers of category items is an innovative and effective analysis method that enables analysts to determine the communication practices of privacy matters and the typical contents of privacy

policies in health care Web sites. This explorative study is intended to help customers, software engineers, and privacy managers understand how privacy policies are expressed on health care Web sites.

When new technologies are adopted, an organization's privacy policy must be revisited and oftentimes revised to respond to policy conflicts introduced by these new technologies. It is important to think of privacy in terms of customers' interest but also companies' interest. The conception of this dissertation encourages informed consent and fosters the development of practical, fine-grained, and sensitive policies for protecting privacy. The development of privacy practices is a very quality-dependent issue, because there are so many principles, categories, and situations to consider. It is relatively easy to set up a Web site, but far more difficult to create a web-based business model. Trustworthy privacy practices should become an obviously imperative source of value creation and competitiveness, and despite their underlying importance for the functioning and organization of e-commerce, the optimum result has not yet been achieved. The results reported here present evidence regarding the need for effective privacy practice management, because

- from the perspective of privacy, confidentiality and trust, customers need more comprehensible tools to gain control over organizations' privacy policies and practices; and
- from the perspective of information and communication technology design, companies need more comprehensible methods for the development of organizations' privacy policies and practices.

In the Internet context, customers rarely deal directly with any person and therefore customers depend on an impersonal electronic storefront to act on their behalf. The results reported here are expected to provide additional benefits to privacy managers, software engineers, and customers by providing more objective criteria for evaluating a Web site's privacy practices. This thesis has many practical implications for the ways in which organizations increase privacy quality and consumer trust, and thereby increase the willingness of prospective customers to use Internet services. Since perceptions of the reputation of a health provider are important to the level of consumer trust in it, online health providers should do what they can to impress prospective customers with these privacy aspects of their operation. Web sites should be set up to encourage business, not to preclude it. If prospective customers cannot easily find what they are looking for on a health care Web site, they may move on to find another site that makes its informational and interactive content more apparent.

Considering the balanced privacy model, it seems that we will fail if we pursue one permanent privacy policy content. According to the balanced privacy model, flexibility and interactivity are important issues to consider due to the Privacy-on-Demand and the Service-on-Demand functions. While we are waiting more sophisticated applications, online companies are already able to "*easily*" express their privacy practices more understandably and design them to call attention to the nature and significance of the privacy situation using the category schemes presented in this dissertation. Since the balanced privacy model seems to be a suitable business model for e-commerce, we need techniques to construct it. In that setting, the major category scheme (i.e. the protective and vulnerability categories) and the visibility category scheme (i.e. the visible and invisible categories) would play a central role. Additionally, we have learned that privacy rules stem from, and are constrained by, the different modularity categories: legal, technical, business, social, and contractual. All those category schemes provide properties and possibilities for the proposed privacy process model, which is aimed to helping corporate privacy managers consider the different implications of the privacy policies and practices for which they are responsible.

The contribution of the major categorization scheme is primarily intended for privacy managers and consumer advocates. One target of a successful privacy process is to make privacy policies more clear and understandable. Policy makers need to realize that protective and vulnerability privacy matters play a major role in privacy management and privacy policy. The core value framework, the balanced privacy framework, and the balanced privacy model provide arguments for the assessment of privacy practices. According to the study, there is a need for organizations to standardize the way in which they focus on and express their privacy practices. The major category scheme would facilitate the use and the development of privacy policy keyword terminology. The list of formally defined keywords provides a useful and extensible vocabulary, because they standardize what different policies express with different terms in a manner that can increase understanding for consumers (and researchers).

The contribution of the visibility categorization scheme is primarily intended for software engineers, and consumer advocates. Software engineers need to realize that the interplay between visible and invisible methods in the protective and vulnerability settings plays a critical role in privacy management and privacy policy. Assessing existing policies and the requirements for their position within the visibility categorization scheme aids software engineers as they seek ways in which to better inform Web site users

about privacy practices, and ways in which to minimize existing and potential information vulnerabilities. The core value framework, the balanced privacy framework, and the balanced privacy model indicate the target direction of Web site development. In other words, the most desirable kind of Web site is one that emphasizes consumer trust and protection by implementing visible and protective items. The primary challenge is how to convert invisible and vulnerability items into visible and protective items. However, it is not possible to convert all vulnerability items into protective items. Therefore, at a minimum it is important to convert invisible items into visible items to support the Privacy-on-Demand and Service-on-Demand functions. The Internet can be used to build not only closer but also more trustworthy relationships with customers. The interactivity possibilities of the Internet provide many ways to manage privacy practices, thus allowing customers to make the most convenient choices from the alternatives, with consideration to their own needs and values, also over cultural boundaries.

The contribution of the modularity category scheme refers to the capacity to view things in light of their true relations or relative importance. The modularity category scheme seeks to help privacy managers maintain a holistic view of privacy within the context of their organizations in tandem with how those categories constrain and influence information practices. When employed to create a privacy policy, the modularity category scheme will ensure that privacy managers adopt a more holistic view of the organization's information practices. Privacy policies should express organizational values and beliefs that relate to organizational success factors, as well as customers' privacy concerns that are reflected directly through their thoughts and actions. The privacy process presents the criteria for modifying privacy practices and policies and designing new ones to balance customers' interest in privacy with the benefits of having so much information, and to balance the rights of customers to privacy against the desire of companies to use this technology to improve their marketing and to better target their products to the interests of customers. The scheme demonstrates that the framework also provides a useful modular basis for analyzing and comparing privacy situations. The modularity categories offer a foundation for reasoning about health provider and Internet privacy policy and privacy management from the viewpoints of the balanced privacy model.

The contribution of the modularity category scheme refers to the privacy process and the layered privacy model. In a situation where corporations and organizations are struggling to handle an exponential increase in the number of online transactions, to protect the privacy and security of proprietary and

personal data, and to deal with the growing complexity of IT systems, informational privacy issues are not only a matter of legal and technical issues and their mutual interaction. Activities at different levels in the organization typically have different tasks, actions, and goals and the privacy practices therefore vary accordingly. It is neither the kind of data nor the content of the data itself that will determine the privacy matter. Instead, it is the situation in which the knowledge is used that we must consider. Business practices of the Internet call attention to an evolutionary approach to privacy policy development. It also seems that the modularity category scheme entails progress to appropriately consider the privacy situation in the organization from the perspective of actions.

First of all, each category of modularity structure can be considered individually. The importance of each modular category revision may vary between activities. In addition, modularity category schemes provide the opportunity to accomplish the privacy process using different tactics. Secondly, the modularity category scheme is a good basis for revising privacy practice using several specialists. Thirdly, using the modularity category scheme allows the privacy manager make useful checklists. Those checklists help with regard to the scope of the privacy process. Prepared checklists are a step in the direction of clarity and accuracy, but also in the direction of preventing some misunderstandings and failures in advance. Fourthly, the modularity category scheme and the balanced privacy model offer a means and advantages for more customer-friendly privacy policy design. Effective metaphors can be used to express organizational privacy practices and bridge the gap between Web site privacy practices and consumer understanding, thereby increasing their clarity and visibility. Metaphors have the capability to give more basic information to customers. It is proposed that these kinds of practices can be used to deal with metaphors when flexibility is not needed. According to the study, privacy seals do not seem to be the best practices for categories where flexibility and collaborating options are needed. Privacy seals have the potential to provide assurance for some privacy and security matters but not all. The functions of Service-on-Demand and Privacy-on-Demand require richer media for clarification and verbal discussion, at least in the health care context.

5.6 Future Research

Because the applications of information technology are logically malleable, there are sufficient strategic reasons to suggest that privacy management as a concept and practice will survive, and that to ignore privacy issues might be fatal for the success of electronic commerce. If we naively regard the issues of privacy policy as routine or, even worse, as unsolvable, then customers are in the greatest danger of being harmed by information technology or those services will not be used at all. The privacy policy analyses and the theoretical frameworks reported in this dissertation are certainly not a definite evaluation of the content implications of privacy policy. Rather, they are a first step toward exploring privacy practices in electronic commerce.

The research agenda on this topic should include the following:

- A fuller range of privacy policies collected from different business segments should be examined. Given that there have been no systematic content comparisons between privacy policies among different business segments, it would be helpful to know whether content differences are still discernable across the fuller range of health care privacy policies.
- A fuller range of privacy policies collected from different countries should be examined. Given that there have been no systematic content comparisons between privacy policies among different countries, future research could test whether the presented technique is suitable for measuring the differences between different cultures.
- A fuller range of privacy practices collected from inside an organization should be examined. More qualitative privacy practice analyses should be undertaken for testing and validating the balanced privacy model and the layered privacy model. If it is possible to perform the privacy study inside the organization, it is likely to yield knowledge (also tacit knowledge) that is inherently very valid, useful, and relevant to the purposes of the organizational privacy process.

The results of this study should be tested and validated in many business segments. The distinctions between business and health care-related Internet services need more study, since it seems that these have different requirements concerning the privacy. Additional reliability testing would enhance the reliability of the presented category and theoretical frameworks, and make generalization and a formal theory effort more rigorous. "*Any substantive theory evolves from the study of a phenomenon situated in one particular situational context. A formal theory emerges from a study of a phenomenon*

examined under many different types of situations." (Strauss and Corbin, 1990, p. 174).

The objective of the future study is to examine cultural and business adaptation on the Web and provide insights to Web marketers on developing Web sites and privacy practices that are not only culturally but also globally adapted. This research compares U.S. health care Web sites when studying the privacy practices of Web sites. Future research should include comparisons between the U.S. and EU privacy practices, because the health care sector and services in these markets are clearly organized differently and function in different ways. There are two main solutions to deal with the legitimate rights of informational privacy. The more common is to use the regulatory powers of the state. This practice is predominant in the EU, which uses very strict directives concerning the privacy matter. The other solution is the voluntary basis. That practice is very predominant in the U.S., where the greatest likelihood is that industry will be left to develop voluntary guidelines, rather than Congress imposing regulations. It would be both important and interesting to measure how EU directives and the studied health care privacy policies correlate. Privacy studies are also encouraged for the broader examination of cross-cultural differences among other countries regarding the effects of privacy and trust. "*Studying cultural content on Web sites can also provide insights into the cultural and societal characteristics of a particular national culture and help marketers to avoid cultural faux pas when marketing globally*" (Singh, Zhao and Hu, 2003, p. 73). Studies by Barber and Badre (1998) suggest that country-specific and culturally-sensitive Web content enhances usability, reach, and Web site interactivity, which in turn leads to more Web traffic and business activity on the Web. Thus it is supposed that culturally expressed privacy practices reduce the anxiety associated with a new medium like the Internet. Future research could test whether this local sensitivity can be applied to a global setting using the balanced privacy model and the layered privacy model.

More qualitative privacy practice analyses should be undertaken for testing the balanced privacy model and the layered privacy model. The proposed privacy process and the layered privacy model seem to be an adequate method for evaluating and developing privacy practices in a trustworthy way, thus fostering customers' positive predispositions and converting previous negative experiences into positive attitudes. Inquiry from the inside and inquiry from the outside (Evered and Louis, 1981) can both serve the purposes of privacy practice research, but in different ways and with different effects. If the study can be performed from the inside, it is likely to yield knowledge (also tacit

knowledge) that is inherently very valid, useful, and relevant to the purposes of organizational privacy practices. It is important to understand employee attitudes. Understanding the attitudes of employees, who have access to personal information, will assist the field in developing better methods for privacy protection (Smith, Milberg and Burke, 1996). When we further study the suitability and usefulness of the balanced privacy model and the layered privacy model for the privacy process, we need knowledge and experience from inside the organizations in order to be able to make judgments and evaluations of the privacy process model.

It is important that privacy practices are also studied in the future, because the privacy issues of e-health and electronic commerce will continue to be more important to consumers and Internet companies. This dissertation showed one possible technique regarding the assessment of the content and communication practices of privacy policies in health care Web sites. It is supposed that there are many other interesting and important issues to study in the electronic commerce context, and the presented technique might be a very useful instrument to do that. In order to enhance the reliability of the technique, the author urges future researchers to replicate this study in other communities. However, the author believes that this dissertation will be informative and applicable to privacy managers at companies in the early stages of developing an electronic commerce strategy, and to academicians studying the evolution of electronic commerce initiatives in the health care business. The intention in conducting this research is not to embarrass or single out particular health Web sites or to scare consumers away from getting valuable health information; rather aspires to alert consumers and the industry to impending threats and problems so that the industry can develop a more suitable electronic commerce solution.

REFERENCES

Abbot R.J. (1983). Program Design by Informal English Descriptions. *Communications of the ACM*, 26(11):882-894, November.

Adkinson W.F., J.A. Eisenach and T.M. Lenard (2002). Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites. Washington, DC: Progress & Freedom Foundation, 2002. Downloaded September, 20, 2003: http://www.pff.org/publications/privacyonlinefinaleel.pdf

Alexander J.E. and M.A. Tate (1999). *Web Wisdom: How to Evaluate and Create Information Quality on the Web*. Mahwah, NJ: Lawrence Erlbaum Associates.

Allen A.M. (1995). The New Nutrition Facts Label in the Print Media: A Content Analysis". *Journal of the American Dietetic Association* 95, 349-351.

AMA (2001). American Medical Association, AMA Suggests for a Healthy New Year, Dec.20, 2001, press release.

Anderson D., D. Sweeney and A. Williams (1993). *Statistics for Business and Economics*, 5th ed., 1993, West Publishing Company.

Ansoff H.I. (1979). *Strategic Management*, London, Macmillan.

Antón A.I. (1997). *Goal Identification and Refinement in the Specification of Software-Based Information Systems*, Ph.D. Dissertation, Georgia Institute of Technology, Atlanta.

Antón A.I., J.B. Earp, D. Bolchini, Q. He, C. Jensen, W. Stufflebeam (2003). The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. *NCSU CSC Technical Report* #TR-2003-14, 1 August 2003.

Antón A.I., J.B. Earp and A. Reese (2002). Analyzing Web Site Privacy Requirements Using a Privacy Goal Taxonomy. 10th Anniversary IEEE Joint Requirements Engineering Conference (RE'02), Essen, Germany, 9-13 September 2002.

Antón A.I. and C. Potts (1998). The Use of Goals to Surface Requirements for Evolving Systems, Int'l Conf. on Software Engineering (ICSE '98), Kyoto, Japan, pp. 157-166, 19-25 April 1998.

Babbie, E. (1995). *The Practice of Social Research*. Wadsworth, Belmont CA.

Barber W. and A. Badre (1998). Culturability: The Merging of Culture and Usability. 4th Conference of Human Factors & the Web, Baskin Ridge, New Jersey, June 5, 1998. Available online at: http://www.research.att.com/conf/hfweb/

Bard M. (2002). Manhattan Research the Future of e-Health. The presentation available at http://www.manhattanresearch.com/signsoflife.pdf

Baumer D., J.P. Earp and F.C. Payton (2000). Privacy, Computerization of Medical Records, and the Health Insurance Portability and Accountability Act of 1996, Presented at the Annual Conference of the Pacific Southwest Academy Legal Studies in Business, California, Feb. 24-27, 2000.

Bayer, Cynthia (2004). The Internet and Health Literacy: Moving Beyond the Brochure. In Schwartzberg, J.G., J. VanGeest, C.C. Wang (Editors). *Understanding Health Literacy: Implications for Medicine and Public Health*. (Chicago: AMA Press, 2004).

Belanger F., J.S. Hiller and W.J. Smith (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems*, Vol. 11, 245-270.

Berg B.L. (1998). *Qualitative Research Methods for the Social Sciences*. Allyn & Bacon, Boston, MA.

Berelson B. (1952). *Content Analysis in Communications Research*, Glencoe, IL: Free Press.

Berland G.K. (2001) Health Information on the Internet: Accessibility, Quality, and Readability in English and Spanish, *JAMA*, May 23/30, 2001, vol. 285, No. 20.Available at: http://jama.ama-assn.org/cgi/content/full/285/20/2612

Bigus J. P. (1996) *Data Mining With Neural Networks*. McGraw-Hill, New York.

Bok S. (1983). *Secrets: On the Ethics of Concealment and Revelation*. Vintage Books, New York.

Booch G. (1991). *Object-Oriented Design with Applications*. Benjamin Cummings. Redwood City, California.

Boulding K. (1968). *Beyond Economics*, Ann Arbor, University of Michigan Press.

Bradach J.L. and R.G. Eccles (1989) Markets versus Hierarchies: From Ideal Types to Plural Forms. *Annual Review of Sociology* 15: 97-118.

Brannigan V.M. and B.R. Beir (1995). Patient Privacy in the ERA of Medical Computer Network: A New Paradigm for a New Technology, *Medinfo*, 8 Pt 1:640-643.

Bunker M. (2000). Insurance Site Exposes Personal Data, *MSNBC*, March 22, 2000.

Bynum T. and S. Rogerson (1996) Introduction and Overview: Global Information Ethics. *Science and Engineering Ethics*, 2 (2): 131-136.

Cavoukian A. (1998). Data Mining: Staking a Claim on Your Privacy. *Information and Privacy Commisioner's Report*, Ontario, Canada.

Cheng H. and J.C. Schweitzer (1996). Cultural values reflected in Chinese and U.S. television commercials. *Journal of Advertising Research*, (May/June), 27-45.

Children's Online Privacy Protection Act, COPPA. The Federal Trade Commission's COPPA site at http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/adults.htm

Chiles T. H. and J. F. McMackin (1996). Integrating Variable Risk Preferences, Trust, and Transaction Cost Economics, *Academy of Management Review* 21(1): 73-99.

Chow A., Z. Hudson, J. Pritts and J. Goldman (2001). Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users. Available at: http://www.pewinternet.org/reports/

Chow S. and R. Holden (1997). Toward an Understanding of Loyalty: the Moderating Role of Trust. *Journal of Managerial Issues* 9(3) (Fall 1997): 275-298.

Clemons E.K., and B.W. Weber (1994). Segmentation, Differentiation, and Flexible Pricing: Experience with Information Technology and Segment-Tailored Strategies. *Journal of Management Information Systems* 11, no. 2 (Fall 1994).

Cline, R.J.W. and K.M. Haynes (2001). Consumer Health Information Seeking on the Internet: The State of Art. *Health Educ*. Res. 2001; 16; 671-692.

Coase R.H. (1937). The Nature of the Firms. *Economica* 4, 386-405.

Cowton C.J. (1998a). Research in Real Worlds: The Empirical Contribution to Business Ethics, in Cowton C.J. and R.S. Crisp (eds.) *Business Ethics: Perspectives on the Practice of Theory* (Oxford University Press, Oxford, pp. 97-115.

Cowton C.J. (1998b). The Use of Secondary Data in Business Ethics Research. *Journal of Business Ethics* 17, 423-434.

Cranor L.F., J.Reagle and M.S. Ackerman (1999). Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, *AT&T Labs-Research Technical Report* TR 99.4.3, http://www.research.att.com/library/trs/TRs/99/99.4/99.43/report.htm

Cronin M. (1996). *The Internet Strategy Handbook*. Boston, MA: Harvard Business School Press.

Cross R. (1982). *Economic Theory and Policy in the UK*, Oxford, Martin Robertson.

Culnan M.J. (1999). Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission. Washington, DC: Georgetown University, The McDonough School of Business, available at: http://www.msb.edu/faculty/culnanm/gippshome.html, 1999.

Culnan M.J. and P.K. Armstrong (1998). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*.

Culver C., J. Moor, W. Duerfeldt, M. Kapp, and M. Sullivan (1994). Privacy. *Professional Ethics* 3. Nos. 3 & 4: 3-25.

Daft R.L. and Lengel R.H. (1986). Organizational Information Requirements, Media Richness and Structural Design. *Management Science*, 32(5), 554-571.

Dalton D.R. and M.B. Metzger (1992). Towards Candor, Cooperative & Privacy in Applied Business Ethics Research: The Randomized Response Technique. *Business Ethics Quarterly* 2, pp. 207-221.

Darr (1997). *Ethics in Health Services Management*, Third Edition, Health Professions Press, Inc. Baltimore, MD.

DeCew J. W. (1997). *In Pursuit Privacy: Law, Ethics, and the Rise of Technology.* Cornell University Prsee, Ithica, NY.

DeCovny S. (1998). The Electronic Commerce Comes of Age. *The Journal of Business Strategy*, Vol. 19, No. 6, pp. 38-44.

Detweiler R.A. (1978). Culture, Category Width, and Attributions. *Journal of Cross-Cultural Psychology*, 9(3), 259-284.

Diaz J., R. Griffith, J. Ng, S. Reinert, P. Friedmann, A. Moulton (2002). Patients' use of the Internet for medical information. *J Gen Intern Med* 2002 Mar;17(3):180-185.

Diesing P. (1971). *Patterns of Discovery in the Social Sciences*. Chicago: Aldine.

Dominick J.R. (1999). Who Do You Think You Are? Personal Home Pages and Self Presentation on the World Wide Web. *Journalism & Mass Communication Quaterly* 77 (Winter 1999): 647.

Doney P.M. and J.P. Cannon (1997), An Examination of the Nature of Trust in Buyer-Seller Relationships, *Journal of Marketing* 61 (April 1997): 35-51.

Drucker P. (1995). *The Post-Capitalist Society*. Oxford: Butterworth-Heinemann.

Earl P.E. and N.M. Kay (1985). How Economists can Accept Shackle's Critique of Economic Doctrines without Arguing Themselves out of their Jobs. *Journal of Economic Studies* 12 (1-2).

Earl M. J. and Ian A. Scott (1999). Opinion What Is a Chief Knowledge Officer? *Sloan Management Review*. Winter 1999.

Earp J.B., A. I. Antón and O.P. Jarvinen (2002). A Social, Technical and Legal Framework for Privacy Management and Policies. *Proceedings of the Eighth Americas Conference on Information Systems* (AMCIS 2002), Dallas, Texas, pp. 605-612, 9-11 August, 2002.

Earp J.B. and D. Baumer (2003). Innovative Web Use to Learn about Consumer Behavior and Online Privacy. *Communications of the ACM*, v.46, n.4, April 2003.

Edelstein H. (1996). Technology How To: Mining Data Warehouses. *Information Week* (January 8).

Edgar S. (1997). *Morality and Machines: Perspectives in Computer Ethics*. Jones and Bartlett Publisher, Sudbury, MA.

Eisenberg A. (1996). Privacy and Data Collection on the Net. *Scientific American* (March), p. 120.

El Sawy O. A., I. Eriksson, A. Raven and S. Carlsson (1999). "Understanding Shared Knowledge Creation Spaces around Business Processes: Precursors to Process Innovation Implementation. *Journal of Technology Management*, 1999.

Electronic Privacy Information Center Alert 7.15, August 3, 2000 (www.epic.org/alert/EPIC_alert_7.15.html).

Ellinger A.E., D.F. Lynch, J.K. Andzulis and R.J. Smith (2003). B-to-B E-Commerce: A Content Analytical Assessment of Motor Carrier Websites. *Journal of Business Logistics*, vol. 24, no 1, 2003. pp 199-220.

Elofson G. (2001). Developing Trust with Intelligence Agents: an Exploratory Study. *Trust and Deception in Virtual Societies*. (Ed.) C. Castelfranchi, Y-H. Tan, 125-138. Kluwer Academic Publishing. Dordrecht.

Eng T.R. (2001). *The EHealth Landscape: A Terrain Map of Emerging Information and Communication Technologies in Health and Health Care*. Princeton, NJ: The Robert Wood Johnson Foundation, 2001.

E-marketer (2001). The eGlobal Report. Available online at: http://www.emarketer.com

Etzioni O. (1996). The World Wide Web: Quagmire or Gold Mine? *Communications of the ACM* (November), 39(11): 65-68.

EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

Evans J.R. and V.E. King (1999). Business-to-Business Marketing and the World Wide Web: Planning, Managing, and Assessing Web Sites. *Industrial Marketing Management*, Vol. 28, No. 3, pp. 343-358.

Evered, R. and M.R. Louis (1981). Alternative Perspectives in the Organizational Sciences: Inquiry from the Inside and Inquiry from the Outside. *Academy of Management Review*, no. 3.

Eysenbach G. and C. Kohler (2002). How Do Consumers Search For And Appraise Health Information on the World Wide Web? Qualitative Study Using Focus Groups, Usability Tests, and In-Depth Interviews. *BMJ* 2002 Mar 9;324(7337):573-577.

Fayyad U., G. Piatetsky-Shapiro and P. Smyth (1996). The KDD Process for Extracting Useful Knowledge from Volumes of Data. *Communications of the ACM*, 39 (11): 27-34.

Ferguson T. (2002) From Patients to End Users. *BMJ* 2002 Mar 9;324(7337):555-556. At http://www.fergusonreport.com/articles/fr00801.htm

Fisher R.J. and J.H White (1976). Intergroup Conflicts Resolved by Outside Consultants. *Journal of the Community Development Society* 7: 88-98.

Flesch R. (1949). *The Art of Readable Writing*, MacMillan Publishing.

Fontanella J. (2000). The Web Based Supply Chain. *Supply Chain Management Review*, Vol. 3, No. 4, pp. 17-20.

Ford R.C. and W.D. Richardson (1994). Ethical Decision Making: A Review of the Empirical Literature. *Journal of Business Ethics* 13, pp. 205-221.

Fox S. (2001a). Fear of Online Crime (2001) at http://www.pewinternet.org/reports/toc.asp?Report=32

Fox S. (2001b). Wired Seniors (Pew Internet & American Life Project Web Site). September 9, 2001. Available at: http://www.pewinternet.org/reports/toc.asp?Report=40 Accessed February 2, 2004.

Fox S. and D. Fallows (2003). Internet Health Resources. Available at: http://www.pewinternet.org/reports/

Fox S. and L. Rainie (2000) The Online Health Care Revolution: How the Web Helps Americans Take Better Care of Themselves. Available at: http://www.pewinternet.org/reports/toc.asp?Report=26

Fox S. and L. Rainie (2002). How Internet Users Decide What Information to Trust When They Or Their Loved Ones Are Sick. http://www.pewinternet.org/reports/toc.asp?Report=59

Fox S., L. Rainie, J. Horrigan, A. Lenhart, T. Spooner, and C. Carter (2000). Trust and Privacy online: Why Americans want to rewrite the rules. http://www.pewinternet.org/reports/toc.asp?Report=19

Francett B. (1997). Data Warehousing Is the Sum of Its Smarts. *Software Magazine* (February 1997).

Frankforth-Nachmias C and D. Nachmias (1996). *Research Methods in the Social Sciences*, 5th edition, Arnold, London.

Franzosi R. (1995). Computer-Assisted Content Analysis of Newspaper. *Quality and Quantity* 29, pp. 157-172.

Frey B.S. (2001). From, Economic Imperialism to Social Science Inspiration, (Ed. Elgar, E.) *Inspiring Economics. Human Motivation in Political Economy*, Cheltenham.

Fried C. (1970). Privacy: A Rational Context. Chap. IX in Anatomy of Values. Cambridge University Press, New York. Reprinted in M.D. Ermann, M.B. Williams and C. Gutierrez, editors, *Computers, Ethics, and Society*, pp. 51-63. Oxford University Press, New York, 1990.

Fried C. (1984). Privacy. *Philosophical Dimensions of Privacy*. Ed. F.D. Schoeman. New York: Cambridge University Press: 203-222.

Friedman M. (1953). *The Methodology of Positive Economics*. Essays in Positive Economics. Chicago: University of Chicago Press.

FTC (1973). The Code of Fair Information Practices, U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, *Computers, and the Rights of Citizens*, viii, http://www.epic.org/privacy/consumer/code_fair-info.html, 1973.

FTC (1998). Privacy Online: A Report to Congress, http//www.ftc.gov/reports/privacy3/, Federal Trade Commission.

FTC (2000). Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress. Federal Trade Commission, 2000.

Fulda J. (1997). From Data to Knowledge: Implications of Data Mining. *Computers of Society*, 27 (4): 28, 1997.

Fulda J. (1998). Data Mining and the Web. *Computers and Society* (March), 28(1): 42-43.

Gallant, J. (1997). Focus Your Site on the Customer. *NetMarketing*. Vol. 82, No. 1, pp. M1-M20.

Ganesan S. (1994). Determinants of Long-Term Orientation in Buyer-Seller Relationships. *Journal of Marketing* 58(2) (April 1994): 1-19.

Gavison R. (1980). Privacy and the Limits of the Law, Yale LawJournal, 89, 1980. Reprinted in D. G. Johnson and H. Nissenbaum, editors, *Computers, Ethics & Social Values*, pp. 332-351. Prentice Hall, Englewood Cliffs, NJ, 1995.

Ghose S. and Wenyu Dou (1998). Interactive Functions and Their Impacts on the Appeal of Internet Presence Sites. *Journal of Advertising Research.* Vol. 38, No. 2, pp. 29-43.

Ghosh S. (1998). Making Business Sense of the Internet. *Harvard Business Review*. Vol. 76, No.2, pp. 126-135.

Glaser B. (1978). *Theoretical Sensitivity*. Mill Valley, CA: Sociology Press.

Glaser B.C. and A.L. Strauss (1967). *The Discovery of Grounded Theory*. Chicago: Aldine Publishing Company, 1967.

Goldman J., Z. Hudson and R.M.Smith (2000). Report on the Privacy Policies and Practices of Health Web Sites, sponsored by the California HealthCare Foundation. January 2000. http://www.chcf.org/documents/ihealth/privacywebreport.pdf

Gotlieb C. C. (1995). Privacy: A Concept Whose Time Has Come and Gone, In D. Lyon and E. Zureik, editors, Surveillance, *Computers and Privacy,* pp. 156-171. University of Minnesota Press, Minneapolis.

Gramm-Leach-Bliley Act of 1999 (2000), 15 U.S.C. §§ 6801-6809.

Guba E.G. and Y.S. Lincoln (1981) *Effective Evaluation*. San Francisco, CA: Jossey – Bass.

Gwartney P.A., L. Fessenden and G. Landth (2002). Measuring the Long-Term Impact of a Community Conflict Resolution Process: A Case Study Using Content Analysis of Public Documents. *Negotiation Journal*. Jan. 2002, 18, 1, pp. 51- 74.

Ha L. and L. James (1998). Interactivity Reexamined: A Baseline Analysis of Early Business WebSites. *Journal of Broadcasting and Electronic Media* 42 (fall 1998), pp. 457-474.

Hagood M.J. (1941). *Statistic for Sociologists* (Reynal & Hitchcock, New York). Quoted in I.L.

Hakim C. (1982). *Secondary Analysis in Social Research: A Guide to Data Sources and Methods with Examples*. Allen & Unwin, London.

Hammer M. and J. Champy (1993). *Reengineering the Corporation, A Manifesto for Business Revolution*. Harper Collins Publisher, New York, 1993.

Harris (2001). *Harris Interactive Health Care News*, vol. 1, Issue31, November 13, 2001.

Harris (2002). *Harris Interactive Health Care News*, vol. 2, Issue8, April 10, 2002.

Harris H. (2001). Content Analysis of Secondary Data: A Study of Courage in Managerial Decision Making. *Journal of Business Ethics*, December, pp: 191-208.

Hawes J. M., K. W. Mast and J. E. Swan (1989). Trust Earning Perceptions of Sellers and Buyers. *Journal of Personal Selling and Sales Management* 9 (Spring 1989):1-8.

Health Insurance Portability and Accountability Act of 1996 (1998), 42 U.S.C.A. 1320d to d-8 (West Supp. 1998). See http://aspe.hhs.gov/admnsimp/index.htm or Federal Register.

Heft P.R., F. Hlubocky and C.K. Daugherty (2003): American Oncologists' Views of Internet Use by Cancer Patients: A Mail Survey of American Society of Clinical Oncology Members. *Journal of Clinical Oncology*: March 1, 2003 vol.21,No.5. Abstract at: http://www.jco.org/cgi/content/abstract/21/5/942

Hempel C. (2001). Privacy, *News and Observer*, 24.9.2001.

Henningham J. (1996). The Shape of Daily News: A Content Analysis of Australia's Metropolitan Newspapers. *Media International Australia* 79, pp. 22-34.

Holsti O.R. (1969). *Content Analysis for the Social Sciences*. Addison Wesley, Reading, MA.

Honeycutt E.D., T.B. Flaherty and K. Benassi (1998). Marketing Industrial Products on the Internet. *Industrial Marketing Management*. Vol. 27, No. 1, pp. 63-72.

Horrigan J.B. and L. Rainie (2002a) Getting Serious Online (Pew Internet & American Life Project: March 2002) Available at http://www.pewinternet.org/reports/toc.asp?Report=55.

Horrigan J.B. and L. Rainie (2002b). Counting on the Internet. http://www.pewinternet.org/reports/toc.asp?Report=80

Houston T. and J. Allison (2002). Users of Internet health information: differences by health status. *J Med Internet Res* 2002 Jun-Nov; 4(3):e7. http://www.jmir.org/2002/2/e7/

Howell J.M. and C.A. Higgins (1990). Champions of Technical Innovation. *Administrative Science Quarterly* 35, pp. 317-341.

Huberman A.M. and Crandall D.P. (1982). Fitting Words to Numbers; Some Approaches to Multisite, Multimethod Research in Educational Dissemination. *American Behavioral Scientist* 26, pp. 62-83.

Huberman A.M. and M.B. Miles (1983). Drawing Valid Meaning from Qualitative Data: Some Techniques of Data Reduction and Display. *Quality and Quantity*, 17 (1983) pp. 281-339.

Huizingh E.K. (2000). The Content and Design of Web Sites: An Empirical Study. *Information & Management*. Vol. 37, No. 3, pp. 123-134.

Häyry M. and T. Takala (2001). Genetic Information, Rights, and Autonomy. *Theoretical Medicine* 22: 403-414, 2001.

INF (2001). Privacy Advocates Lobby New AG, *Information Security*, May 2001.

Inmon W.H. (1996). The Data Warehouse and Data Mining. *Communications of the ACM* (November), 39(11): 49-50.

Insch G.S., J.E. Moore and L.D. Murphy (1997). Content Analysis in Leadership Research: Examples, Procedures, and Suggestions for Future Use. *Leadership Quarterly* 8, pp. 1-25.

Jamal K. and N.E. Bowie (1995). Theoretical Considerations for a Meaningful Code of Professional Ethics. *Journal of Business Ethics* 14, pp. 703-714.

Janda K. (1969). A Microfilm and Computer System for Analyzing Comparative Politics Literature, in G. Gerbner, O.L. Holsti, K. Krippendorff, W.J. Paisley and P.J. Stone (eds.), *The Analysis of Communication Content*. Wiley, New York, pp: 407-435.

Janis I.L. (1965). The Problem of Validating Content Analysis, in H.D. Lasswell, N.C. Leites and Associates (eds.). *Language of Politics; Studies in Quantitative Semantics*. MIT Press, Cambridge, MA, pp: 55-82.

Jarvenpaa S. L., N. Tractinsky and M. Vitale (2000). Consumer Trust in an Internet Store, *Information Technology and Management* 1: 45-71.

Jefferson, M. (1983). Economic Uncertainty and Business Decision Making, in Wiseman J. (ed.), *Beyond Positive Economics?* London, Macmillan.

Järvinen O.P., J.B. Earp, and A. I. Antón (2002). A Visibility Categorization Scheme for Privacy Management Requirements. Second Symposium in Requirements Engineering for Information Security, Raleigh, NC, USA, October, 2002.

Järvinen, O.P. (1999). *Usability of Information Systems: Studies in a Hospital Environment*. Licentiate thesis, University of Turku, 1999.

Järvinen O.P. (2003a) Privacy Seal Programs and Privacy Policies in Health Care IT-Services. *Proceedings of the Combining views from IS and service research seminar*, Turku. TUCS General Publication, No 25, June 2003, pp. 41 - 65.

Järvinen O.P. (2003b) Revision of Privacy Policy: Five Perspectives and ONION-model. *People and Computers: Twenty-one Ways of Looking at Information Systems*. (ed. Järvi, T. & Reijonen P.) TUCS General Publication, No 26, June 2003, pp. 167 – 184.

John G. (1984). An Empirical Investigation of Some Antecedents of Opportunims in a Marketing Channel. *Journal of Marketing Research* XXI (August 1984: 278-289.

Johnson D. G. (1994). *Computer Ethics*.2nd ed. Prentice Hall, Englewood Cliffs,NJ.

Kabanoff B., R. Waldersee and M. Cohen (1995). Espoused Values and Organizational Change Themes. *Academy of Management Journal* 38, pp: 1075-1104.

Kaplan A. and J.M. Goldsen (1965). The Reliability of Content Analysis Categories, in *H.D.*

Kassarjian H.H. (1977). Content Analysis in Consumer Research. *Journal of Consumer Research*, 4 (June), 8-18.

Katz v. U.S., 389 U.S. 347 (1967).

Keen P.G.W. (1997). Are You Ready for Trust Economy, *ComputerWorld* 31(16) (April 21 1997): 80.

Kleind B.A. (2001). *Strategic Electronic Marketing: Managing E-B*usiness. Cincinnati, OH: South-Western College Publishing.

Klimas J. (1997). Reengineering in the Real World. *Management Accounting*, May 1997.

Kolbe R.H. and M.S. Burnett (1991). Content-Analysis Research: An Examination of Applications with Directives for Improving Research Reliability and Objectivity. *Journal of Consumer Research*. Vol. 18, No. 1, pp. 243-250.

Kortteinen B., M.I. Nurminen, P. Reijonen and V. Torvinen (1995). Improving IS Deployment through Evaluation: Application of the Onion Model, 3rd European Conference on the Evaluation of IT, Bath University, pp. 175-181.

Kreps D.M. (1997). Intrinsic Motivation and Extrinsic Incentives. *American Economics Review*, Papers and Proceedings.

Krippendorff K. (1980). *Content Analysis*. Sage Publications, Beverly Hills, CA.

Lamsweerde A. van (2001). Goal-Oriented Requirements Engineering: A Guided Tour, IEEE 5th Int'l Symp. on Requirements Engineering (RE'01), Toronto, Canada, pp. 249-261, 27-31 August 2001.

Landro I. (2000). More People Are Using Internet Health Sites, But Fewer Are Satisfied. *Wall Street Journal*. December 29, 2000:9.

Langlois R.N. and P.L. Robertson (1995). *Firms, Markets and Economic Change. A Dynamic Theory of Business Institutions*. Routledge, London.

Laudon K. C. and J. P. Laudon (1999). *Essentials of Management Information Systems. Transforming Business and Management*. Prentice Hall, New Jersey.

Laurel B. (1991). *Computers as Theatre*. Reading, MA: Addison-Wesley, 1991.

Leavitt H.J. (1965). Applied organizational change in industry: structural, technological and humanistic approaches, in: *Handbook of organizations*, edited by J.G. March. Chicago: Rand McNally, 1965.

Lenhart, Amanda (2003). Ever-Shifting Internet Population. (Pew Internet & American Life Project: April 2003) Available at http://www.pewinternet.org/reports/toc.asp?Report=88.

Lenhart A, J. Horrigan and D. Fallows (2004). Content Creation Online. http://www.pewinternet.org/reports/toc.asp?Report=113

Lohse G.L. and P. Spiller (1998). Electronic Shopping. *Communications of the ACM* 41(7) (July 1998): 81-87.

Luhmann N. (1979). *Trust and Power*. John Wiley and Sons.

Luo X. (2002). Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory. *Industrial Marketing Management*, Vol. 31, 111-118.

Lyon D. and E. Zureik (1995). Surveillance, Privacy and the New Technology. In D. Lyon and E. Zureik, editors, *Surveillance, Computers and Privacy*, pp. 1-18. University of Minnesota Press, Minneapolis.

Mason J.K., McCall, and R.A. Smith (1999). *Law and Medical Ethics*. Fifth edition. London, Butterworths, 1999.

Mason R.O. (1986). Four Ethical Issues of the Information Age, *Management Information Systems Quarterly*, Vol. 10, Number 1, March, 1986.

Mayer R.J., J.H. Davis and F.D. Schoorman (1995). An Integrative Model of Organizational Trust, *Academy of Management Review* 20: 709-734.

McAllister D. J. (1995). Affect- and Cognition-based Trust as Foundation for Interpersonal Cooperation in Organizations. *Academy of Management Journal* 38(1): 24-59.

McArthur R. L. (2001). Reasonable Expectation of Privacy, *Ethics and Information Technology* 3: 123-128.

McGlynn E.A., S.M. Asch, J. Adams, J. Keesey, J. Hicks, A. DeCristofaro and E.A. Kerr (2003). The Quality of Health Care Delivered to Adults in the United States. *New England Journal of Medicine*: June 26, 2003 – Vol. 348, No.26.

McKinnon, J. (1988). Reliability and Validity in Field Research: Some Strategies and Tactics. *Accounting, Auditing and Accountability Journal,* vol. 1.

Memon N. and P.W. Wong (1999). Protecting Digital Media Content, *Communications of the ACM*, 41(7), pp. 35-43, Jul. 1999.

Michelfelder D. P. (2001). The Moral Value of Informational Privacy in Cyberspace, *Ethics and Information Technology* 3: 129-135.

Mold J., J. Cacy and E. Barton (1998). Patient-physician Email communication. *Oklahoma State Medical Association*. Sep; 91(6): 331-334.

Moor J. (1990). Ethics of Privacy Protection. *Library Trends* 39 1&2: 69-82.

Moor J. H. (1997). Towards a Theory of Privacy in the Information Age. *Computers and Society*, 27 (3): 27-32.

Moor J. H. (1998). Reason, Relativity, and Responsibility in Computer Ethics. *Computers and Society* (March), 28(1): 14-21.

Morgan R. M. and S.D Hunt (1994). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing* (July 1994): 20-38.

Mueller B. (1987). Reflections of Culture: An Analysis of Japanese and American Advertising Appeals. *Journal of Advertising Research*, (June/July), 51-59.

Neuman W.L. (1994). *Social Research Methods*, 2nd edition. Allyn & Bacon, Boston, MA:

Nissenbaum H. (1997). Can We Protect Privacy in Public? *Proceedings of the Conference on Computer Ethics: Philosophical Enquiry* (CEPE '97), pp. 191-204. Erasmus University, Rotterdam, The Netherlands.

Nonaka I. (1991). The Knowledge-Creating Company. *Harvard Business Review*, volume 69, November-December, pp. 96-104.

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, Vol. 5, No. 1, pp 14-37.

North D.C. (1990). *Stability and Change in Economic History. Institutions, Institutional Change and Economic Performance*. Cambridge University Press, Cambridge.

Nurminen M. and Järvinen O. (2001). Power and Limits of Process Thinking in Health Care. In Björnestad S., R. Moe, A. Mörch, and A. Opdahl (eds.) *Proceedings of the 24th Information Systems Research Seminar in Scandinavia*, Norway, vol 1, 215-224, August, 2001.

N&O (2002). "Privacy", *News and Observer* 24.9.2001.

Olsen P. (2001). Companies rethink Net privacy after attacks. October 2, 2001. http://news.cnet.com/news/0-1005-202-7375378.html

O'Connor K. and A.A. Adams (1999). Research Report: What Novices Think About Negotiation: A Content Analysis of Scripts. *Negotiation Journal*, April, pp: 135-147.

O'Harrow R. (2001) Prozac Maker Reveals Patient Email Addresses, *Washington Post*, July 4, 2001, at E1.

Papacharissi Z. (2002). The Presentation of Self in Virtual Life: Characteristics of Personal Home Pages. *Journalism and Mass Communication Quarterly.* Autumn 2002, 79, 3, pp. 643-660.

Pearson H. P. (2003). Privacy in an on Demand World. A presentation at North Carolina State University, Centennial Campus, April 25, 2003, Raleigh, North Carolina, USA. At http://ecommerce.ncsu.edu/seminar/pearson.html

Perreault W.D. and L.E. Leight (1989). Reliability of Nominal Data Based on Qualitative Judgements. *Journal of Marketing Research* 26 (May 1989), pp. 135-148.

Perry M. and C. Bodkin (2000). Content Analysis of Fortune 100 Company Web Sites. *Corporate Communications: An International Journal*. Vol. 5, No. 2, pp. 87-96.

Peterson R.A., S. Balasubramanian and B.J. Bronnenberg (1997). Exploring the Implications of the Internet for Consumer Marketing, *Journal of the Academy of Marketing Science* 25(4): 329-346.

Pitofsky R. (2000a). Privacy online: Fair information practices in the electronic marketplace. At http://www.ftc.gov.os./2000.05/testimonyprivacy.htm

Pitofsky R. (2000b). Letter from members of Congress to the Honorable Robert Pitofsky, Chairman of the FTC, Feb. 2, 2000, available at http://www.house.gov/commerce_democrats/press/1061tr84.htm)

Porter M. (1985). *Competitive Advantage*. New York: Free Press, 1985.

Porter M. and V. Millar (1995). How Information Gives You Competitive Advantage. *Harvard Business Review*, July-August 1995.

Posner R.A. (1992) *Economic Analysis of Law*. Little, Brown and Co., Boston.

Prince F. (2001). Translating Security for Managers, *Information Security*, May 2001.

Princeton (1999). Confidentiality of Medical Records: National Survey, conducted by the Princeton Survey Research Associates for the California HealthCare Foundation, January 1999. http://www.geocities.com/hdsarmc/records.htm

Princeton (2002). A Matter of Trust: What Users Want From Web Sites. Available at: http://www.consumerwebwatch.org/news/1_abstract.htm.

P3P (2002). P3P Public Overview. Accesses June 24, 2002 at http://www.w3.org/P3P/

Quelch J.A. and L.R. Klein (1996). The Internet and International Marketing, *Sloan Management Review* (Spring 1996): 60-75.

Rachels J. (1975). Why is Privacy Important? Philosophy and Public Affairs, 12 (4). Reprinted in D. G. Johnson and H. Nissenbaum, editors.

Computers, Ethics & Social Values, pp. 351-357. Prentice Hall, Englewood Cliffs, NJ, 1995.

Rafaeli S. (1988). Interactivity: From New Media to Communication. In advancing *Communication Science: Merging Mass and Interpersonal Process*, ed. R. Hawkins et al. Newbury Park, CA: Sage, 1988, pp. 100-134.

Rainie L. (2002). Health Care and the Internet Survey. The Pew Internet & American Life Project 2002 Aug 22. URL: http://www.pewinternet.org/reports/pdfs/PIP_Health_Questionnaire.pdf [accessed 2002 Dec 29]

Randall D.M. and M.F. Fernandes (1991). The Social Desirability Response Bias in Ethics Research. *Journal of Business Ethics* 10, pp: 805-817.

Randall D.M. and A.M. Gibson (1990). Methdology in Business Ethics Research: A Review and Critical Assessment. *Journal of Business Ethics* 9, pp: 457-471.

Regan P. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, Chapel Hill, NC.

Rindfleish T.C. (1997). Privacy, Information Technology, and Health Care, *Communications of the ACM*, August 1997, pp 92-100.

Robertson D.C. (1993). Empiricism in Business Ethics: Suggested Research Directions. *Journal of Business Ethics* 12, pp: 585-599.

Rogers E.M. (1995). *Diffusion of Innovations*. New York: Free Press, 1995.

Rumbaugh J., M. Blaha, W. Premerlani, F. Eddy and W. Lorensen (1991). *Object-Modeling and Design*, Prentice Hall, New York, NY.

Saarinen E. (1956). Time Magazine, July the 2nd.

Sarantakos S. (1993). *Social Research*. MacMillan Australia, South Melbourne.

Schneier B. (1996). *Applied Cryptography : Protocols, Alcorithms and Source Code in C*, Second ed., New York: Wiley.

Schwab D. (2001). Merck sells $1B Worth of drug online. *The Star-Ledger*, Oct. 16, 2001.

Sciamanna C.N., M.A. Clark, T.K. Houston, and J.A. Diaz (2003). Unmet needs of primary care patients in using the Internet for health-related activities. *Journal of Medical Internet Research*: January 8, 2003. Available at: http://www.jmir.org/2002/3/e19/index.htm

Sheenan K.B. and T.W. Gleason (2001) Online Privacy: Internet Advertising Practioners Knowledge and Practises. *Journal of Current Issues and Research in Advertising*, Vol. 23, no. 1, 31-41.

Silverman D. (1993). *Interpreting, Qualitative Data: Methods for Analyzing Talk, Text and Interaction*. Sage Publications, Thousands Oaks, CA.

Simon H.A. (1969). *The Sciences of the Artificial*, Cambridge, Massachusetts, MIT University Press.

Singh N., H. Zhao and X. Hu (2003). Cultural Adaptation on the Web: A Study of American Companies' Domestic and Chinese Websites. *Journal of Global Information Management*, Jul-Sep 2003, 11, 3.

Sipple v. Chronicle Publishing Co. 154 *Cal App*. 3rd 1040 (1984).

Sitkin S. and N.L Roth (1993). Explaining the Limited Effectiveness of Legalistic Remedies for Trust/Distrust. *Organization Science* 4(3): 367-392.

Slovic P. (1999). Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. *Risk Analysis* 19: 689-701, 1999.

Smith J. B. and D. W. Barclay (1997). The Effects of Organizational Differences and Trust on the Effectiveness of Selling Partner Relationships. *Journal of Marketing* 61 (January 1997): 3-21.

Smith, H.J., S.J. Milberg and S.J. Burke (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practises, *MIS Quarterly*, June 1996, pp. 167-196.

Smolla R. A. (1992). *Free Speech in an Open Society*. Vintage/Random House, New York.

Somerville A. (1999). English V. Genetic Privacy: Orthodoxy or Oxymoron? *Journal of Medical Ethics*, 1999; 25: 144-150.

Spooner T and L. Rainie (2001a). Hispanies and the Internet (Pew Internet & American Life Project Web site) July 25, 2001. Available at: http://www.pewinternet.org/reports/toc.asp?Report=38 Accessed February 2, 2004.

Spooner T and L. Rainie (2001b). African-Americans and the Internet (Pew Online Life Report Web site) October 22, 2001. Available at:http://www.pewinternet.org/reports/toc.asp?Report=25 Accessed February 2, 2004.

Star L. (1991). The Sociology of the Invisible: The Primacy of Work in The Writings of Anselm Strauss. *Social Organization and Social Process, Essays in Honor of Anselm Strauss*. Aldine De Gruyter, New York, 1991.

Sterrett, C. and A. Sham (1998). Going Global on the Information Super Highway. S*.A.M. Advanced Management Journal*. Vol. 63, No. 1, pp. 43-48.

Strauss A. (1985). Work and the Division of Labor. *Sociological Quarterly*, 16, pp. 1-19.

Strauss A.L. (1987). *Qualitative Analysis for Social Scientists*. Cambridge University Press, New York.

Strauss A. (1988). The Articulation of Project Work: An Organizational Process. *The Sociological Quarterly*, Vol. 29, Number 2, 1988.

Strauss A.S. Fagerhaugh, B. Suczek and C. Wiener (1988). *Articulation Work, Social Organization of Medical Work.* The University of Chigaco Press, 1985.

Strauss A. and J. Corbin (1990). *Basics of Qualitative Research. Grounded Theory Procedures and Techniques*. Sage: New York.

Suchman L. (1987). *Plans and Situated Action*. Cambridge, UK: Cambridge University Press.

Sullivan B. (2000). Bank Information Exposed Online, *MSNBC*, January 19, 2000.

Tavani H.T. (1999a). Informational privacy, data mining, and the Internet, *Ethics and Information Technology* 1: 137-145.

Tavani H.T. (1999b). KDD, Data Mining, and the Challenge for Normative Privacy, *Ethics and Information Technology* 1: 265-273.

Thibaut J.W. and H.H. Kelley (1959). *The Social Psychology of Groups*. Wiley, New York.

Thompson P.B. (2001). Privacy, Secrecy and Security, *Ethics and Information Technology* 3: 13-19.

Thompson P.B. (1999). The Ethics of Truth-Telling and the Problem of Risk, *Science and Engineering Ethics* 5(4): 489-511.

Trevino L.K. (1986). Ethical Decision Making in Organizations: A Person-Situation Interactionist Model. *Academy of Management Review* 11, pp: 601-617.

Tunik M. (1998). *Practices and Principles*. Princeton University Press, Princeton, NJ, pp. 161-190.

Udo G.J. (2001). Privacy and Security Concerns as Major Barriers for Electronic commerce: A Survey Study. *Information Management & Computer Security*, Vol. 9, No. 4, 165-174.

URAC (2001a). Consumers and Health Web Sites. At http:// webapps.urac.org/Websiteaccreditation/Portal/Business/Consumer Value. asp

URAC (2001b). Survey of Consumers' Attitudes Towards Health Web Sites and Accreditation, conducted by Harris Interactive for URAC, May 2001.

Uslaner E.M. (2000). Trust, Civic Engagement, and the Internet. European Consortium for Political Research, University of Grenoble, April 6-11, 2000. Available at: http://www.bsos.umd.edu/gvpt/uslaner/internettrust.pdf

U.S. Supreme Court (1965). At 381 US 49.

Warren S. and L.D. Brandeis (1890). The Right to Privacy. *Harvard Law Review* 4, 193 – 220.

Watson R.T., P. Berthon, L.F. Pitt and G.M. Zinkhan (2000). *Electronic Commerce: The Strategic Perspective*. Forth Worth, TX: The Dryden Press.

Weaver G.R. and L.K. Trevino (1994). Normative and Empirical Business Ethics: Separation, Marriage of Convenience, or Marriage of Necessity? *Business Ethics Quarterly* 4, pp: 129-143.

Weber J. (1992). Scenarios in Business Ethics Research: Review, Critical Assessment, and Recommendations. *Business Ethics Quarterly* 2, pp: 137-159.

Weber R.P. (1990). Basic Content Analysis. *Sage University Paper Series on Quantitative Applications in the Social Sciences* 49. Sage Publications, Beverly Hills, CA.

Whinston A.B., D.O. Stahl, and S.Y. Choi (1997) *The Economics of Electronic Commerce.* MacMillan Technical Publishing, Indianapolis, Indiana.

Wilkins R.G. (1987). Katz v. U.S. *Vanderbilt Law Review*, 40: 1077-1129, October 1987.

Williamson O. E. (1975). *Markets and Hierarchies: Analysis and Antitrust Implications*. NY: Free Press.

Williamson O.E. (1985). *The Economic Institutions of Capitalism. Firms, Markets, Relational Contracting*. Free Press, New York.

Williamson O.E. (1993). Opportunism and its Critics. *Managerial and Decision Economics* 14 (2), 97-107.

Williamson O.E. (2000). The New Institutional Economics: Taking Stocks, Looking Ahead. *Journal of Economic Literature* 38(3), 595-613.

Wilson C. (2001). Lilly Reveals Prozac Patients' Identities. http://www.infobeat.com/cgibin/WebObjects/IBFrontEnd.woa/wa/fullStory?article=409190643

Woodrum J. (1984). Mainstreaming Content Analysis in Social Science: Methodology, Advantages, Obstacles and Solutions. *Social Science Research* 13, pp: 1-19.

Yin, R.K. (1991). *Case Study Research: Design and Methods*, Revised Edition, Applied Social Research Method Series, Vol. 5, Sage Publications, Newbury Park.

Zack M. H. (1999). Managing Codified Knowledge, *Sloan Management Review*, Summer 1999.

Zemke R. and T. Connellan (2001). *E-Service: 24 Ways to Keep Your Customers – When The Competition Is Just A Click Away*. New York: American Management Association.

Zucker L.G. (1986). Production of Trust: Institutional Sources of Economic Structure, 1840-1920, in: *Research in Organizational Behavior*, 8, eds. B.M. Staw and L.L. Cummings (JAI Press, 1986): pp. 53-111.

TURUN KAUPPAKORKEAKOULUN JULKAISUSARJASSA A OVAT VUODESTA 2004 LÄHTIEN ILMESTYNEET SEURAAVAT JULKAISUT

A-1:2004 Sakari Lehtiö
Suomen pankkikriisin taustatekijät, luonne ja kriisinhoito erityisesti säästöpankeissa

A-2:2004 Seppo Ristilehto
Liiketoimintashokki
Tapaustutkimus laivanrakennus- ja autoteollisuusalan yritysten kriisiratkaisuista ja ohjaustoimenpiteistä

A-3:2004 Tomi J. Kallio
Organisaatiot, johtaminen ja ympäristö.
Organisaatiotieteellisen ympäristötutkimuksen ongelmista kohti yleistä teoriaa yritys-luontosuhteesta

A-4:2004 Zsuzsanna Vincze
A Grounded Theory Approach to Foreign-Market Expansion in Newly-Emerging Markets. Two Finnish Companies in the Visegrád Countries

A-5:2004 Anni Paalumäki
Keltaisella johdetut. Artefaktit, johtaminen ja organisaation kulttuurinen identiteetti

A-6:2004 Eila Heinonen
Aktiivinen harrastus työn siirtymän ja kompensaation ilmentymänä. Case matkailuoppaat

A-7:2004 Eija Koskivaara
Artificial Neural Networks for Analytical Review in Auditing

A-8:2004 Karin Holstius and Pentti Malaska
Advanced Strategic Thinking. Visionary Management

A-9:2004 Jari Hyvärinen
Empirical Evidence on International Outsourcing in Production

A-10:2004 Esa Puolamäki
Strategic Management Accounting Constructions in Organisations. A Structuration Analysis of Two Divisional Strategy Processes

A-11:2004 Jani Erola
A Remedy with Rationalities. Improved Rational Action Theory with Empirical Content as a Solution to the Fallacies in Sociology

A-12:2004 Tomi Viitala
Tax Treatment of Investment Funds and Their Investors within the European Union

A-13:2004 Jonna Järveläinen
Online or Offline: Motives behind the Purchasing Channel Choice of Online Information Seekers

A-14:2004 Aapo Länsiluoto
Economic and Competitive Environment Analysis in the Formulation of Strategy. A Decision-Oriented Study Utilizing Self-Organizing Maps

A-15:2004 Pekka Stenholm
Maantiekuljetusyrityksen ympäristölähtöinen kilpailukyky

A-16:2004 Juha Kontio
Diffusion of Database Innovations. A Multiple Case Study in Six Finnish Organizations

A-1:2005 Satu Rintanen
The Establishment and Development Directions of Corporate Environmental Management – Case Studies in Italian and Finnish Meat Processing Sector

A-2:2005 Seppo Määttä
Strategian ja strategisen informaation tulkintahorisontteja. Case Valtiovarainministeriö

A-3:2005 Olli Järvinen
Privacy Management of e-Health. Content Analysis of 39 U.S. Health Providers' Privacy Policies

Kaikkia edellä mainittuja sekä muita Turun kauppakorkeakoulun julkaisusarjoissa ilmestyneitä julkaisuja voi tilata osoitteella:

KY-Dealing Oy
Rehtorinpellonkatu 3
20500 Turku
Puh. (02) 481 4422, fax (02) 481 4433
E-mail: ky-dealing@tukkk.fi

All the publications can be ordered from

KY-Dealing Oy
Rehtorinpellonkatu 3
20500 Turku, Finland
Phone +358-2-481 4422, fax +358-2-481 4433
E-mail: ky-dealing@tukkk.fi