

# A Social, Technical and Legal Framework for Privacy Management and Policies

**Julia B. Earp**  
North Carolina State University  
julia\_earp@ncsu.edu

**Annie I. Antón**  
North Carolina State University  
aiananton@eos.ncsu.edu

**Olli Jarvinen**  
University of Turku  
olli.jarvinen@tukkk.fi

## ABSTRACT

*Organizational privacy policies and privacy practices reflect an organization's perceived trustworthiness to those with which it conducts business. This paper proposes a framework, based upon an in-depth two-year analysis of Internet privacy policies, for examining an organization's privacy management practices within the context of their respective privacy policies. The framework aids in evaluating privacy from various organizational perspectives: legal, technical, business rules, social norms and contractual norms. It also provides assistance when developing privacy policies for e-commerce Web sites. We discuss a case study in which the framework was employed to analyze 23 Internet health care Web site privacy policies.*

**KEYWORDS:** Privacy management, information privacy, privacy requirements and policy.

## 1 INTRODUCTION

The ability for enterprises to reach customers worldwide is creating new opportunities. The Internet already links companies to tens of millions of customers around the world and has become an effective technology for businesses because it offers a straightforward means to interact with other businesses and individuals at a very low cost. Additionally, Web sites are available to consumers 24 hours a day at their convenience.

Today's global economy offers consumers unprecedented access to a wide range of goods and services. Changes have been observed in many sectors, including health care. Health care companies can no longer expect the services and 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. Several analyses (described in Section 3) that focus on health care organizations have guided the development of the framework presented in this paper. The framework incorporates several organizational perspectives that impact privacy policy content as well as privacy management practices. Additionally, it is effective for examining how Web sites claim they manage online customer data and for reasoning about the privacy relationships (e.g. constraining, supporting, conflicting, etc.) between policy statements.

Sound data management practices are essential for organizations that participate in online business due to both the capability to easily collect and use personal information as well as the implications thereof. Any organization embarking upon online transactions should therefore be prepared to address privacy matters and adjust its policy accordingly. 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. Information technology (IT) practitioners need to be aware of the interplay among these perspectives and realize that each plays a critical role in privacy management and privacy policy. The framework presented in this paper addresses these five perspectives and aims to provide a conceptual framework for responsible and efficacious privacy management.

## 2 PRIVACY POLICY

A privacy policy comprehensively describes a Web site's information practices and is located on the site in an easily accessible position (FTC 1998, FTC 2000). 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 e-commerce transactions has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. 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.

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 2002). However, a privacy policy should directly reflect an organization's privacy rules and practices no matter what business function uses the information. Privacy rules stem from, and are constrained by, the following organizational perspectives: legal, technical, business, social and contractual. This paper proposes a framework to aid corporate privacy officers consider the legal, technical, business, social and contractual implications of the privacy policies and practices for which they are responsible. Privacy policies and privacy practices reflect ethical views of an organization and therefore, provide an indication of perceived trustworthiness to those who conduct business with a given organization. This paper seeks to increase the IT community's understanding of privacy policy as a significant trust indicator for fair business practices.

## 3 FRAMEWORK FOR PRIVACY POLICIES AND PRIVACY MANAGEMENT

In this section, we introduce our privacy framework that expresses the five organizational perspectives that must be considered when formulating and/or evaluating an organization's privacy policy and privacy management. These perspectives reflect contractual commitments between organizations, social relationships between users and the organization, motivations of business, technology's capabilities, and the whole of these encompassed within health care and Internet legislations. Before introducing the framework, we discuss the evolution of this research to establish the context and introduce the vocabulary for the discussion in Section 3.2.

### 3.1 Framework Evolution

The framework was developed in conjunction with an in-depth two-year analysis of Internet privacy policies (Antón and Earp. 2001; Antón et al. 2002). The framework is the culmination of several phases of privacy policy and legal analyses based upon our use of the Goal-Based Requirements Analysis Method (Antón 1996; Antón and Potts, 1998). *Goals* are the objectives and targets of achievement for a system. In software engineering, goal-driven approaches for requirements focus on why systems are constructed, expressing the rationale and justification for the proposed system (van Lamsweerde 2001). Goals are a cogent unit by which to objectively analyze and compare Internet privacy policies, enabling us to provide useful guidance to IT practitioners, policy makers, and consumers (Antón and Earp, 2001). A discussion of goal-driven analysis is outside the scope of this paper; interested readers are referred to (Antón 1996; Antón and Potts, 1998, van Lamsweerde 2001).

The framework presented in this paper resulted from our previous experience in analyzing nearly 50 Internet privacy policies (Antón and Earp, 2001), a portion of the European Union Directive<sup>1</sup>, and a European Recommendation addressing Internet privacy.<sup>2</sup> Our analysis began with a goal-based analysis of the latter two legislative documents; each was examined and all privacy-related legal goals were extracted and documented. This analysis was coupled with our analysis of 16 health care Web site privacy policies based upon the privacy goal taxonomy in (Antón et al. 2002). This privacy goal taxonomy classifies privacy goals as either privacy protection goals or privacy goal obstacles that suggest the potential and vulnerability for privacy invasions. Privacy protection goals relate to the *desired protection* of consumer privacy rights, whereas privacy goal obstacles relate to *existing threats* to consumer privacy. Privacy protection goals correspond to the five Fair Information Practice Principles<sup>3</sup>: 1) notice / awareness, 2) choice / consent, 3) access / participation, 4) integrity / security, and 5) enforcement / redress. In contrast, privacy goal obstacles represent statements of fact that suggest the existence of vulnerabilities for privacy invasions.

### 3.2 Privacy Framework Overview

Several researchers have provided various approaches to creating sufficient data protection for consumers. Many of these approaches outline technical measures for providing better security, which in turn provide a higher potential for data privacy (Brannigan and Beir, 1995; Memon and Wong, 1999; Schneier, 1996). Rindfleisch (1997) prescribes privacy, confidentiality and security as the three primary concepts when considering data protection in health care organizations. These three elements are vital for effective data protection, but it lacks a much needed mechanism to evaluate the privacy element in more detail. The privacy goal taxonomy discussed in Section 3.1 provides a good foundation; however, it quickly became apparent to our analysis team that a richer framework was needed to adequately consider privacy within a broader organizational context. We now discuss each of the perspectives that comprise this organizational privacy framework. The legal perspective, in a sense, constrains the technical measures, business rules, social norms and contractual norms of an organization. The technical perspective 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 perspective is contained within the legal perspective because legislation provides the minimum requirement of business practices, thus, business goals must pass through the legal and technical filters. The business perspective thus forms the foundation of the framework as business goals are motivated by social and contractual norms and expectations between organizations and users. The focus of social perspective is on relationships with consumers while the focus of contractual perspective is on contractual relationships with other partnering organizations (e.g. third parties).

These perspectives and their relationships are illustrated in Figure 1. The three inner boxes, labeled users, organization and third parties represent the stakeholders that are influenced and/or constrained by the five perspectives. The relationship between an organization's Web site users and the organization is characterized as social in nature. Organizations and their users (or consumers) interact in a cooperative way, exchanging goods, services and or information. In contrast, the relationship between the organization and its business partners (or third parties if one prefers to employ the standard Internet privacy policy vocabulary) is characterized as contractual. The social and contractual relationships that exist between an organization and the constituent stakeholders are

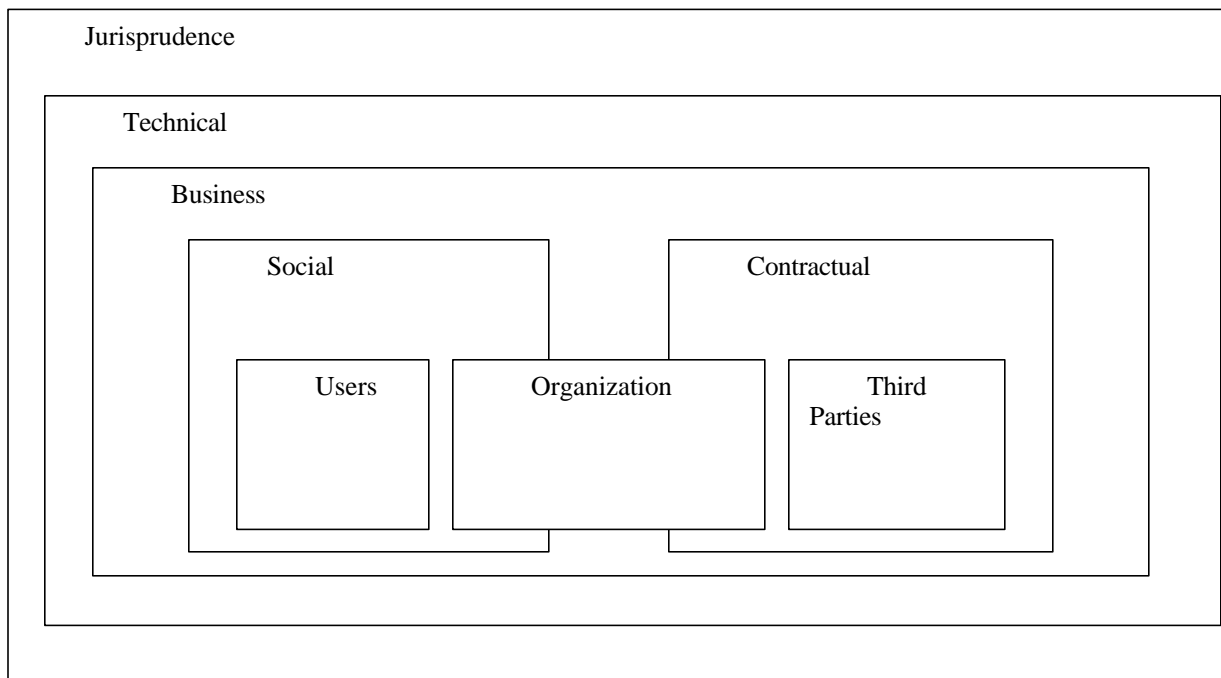
---

<sup>1</sup> DIRECTIVE 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy the telecommunications sector Official Journal L 024 , 30/01/1998 p. 0001 - 0008 23

<sup>2</sup> 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>

<sup>3</sup> 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](http://www.epic.org/privacy/consumer/code_fair_info.html), 1973.

influenced, in turn, by business objectives, technical constraints and most actively by the legal obligation to adhere to relevant legislation.



**Figure 1: Framework for Privacy Management and Policies**

All five perspectives play a key role in the framework especially when one considers that one weak link in the series of perspectives can cause online organizations to become 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 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. We now discuss a case study in which we applied this framework, and then expand by providing detailed descriptions for each perspective in Section 4.

### 3.3 Case Study

To date the framework has been validated via its application in the analysis of 23 health care Web site privacy policies. The five perspectives were used to classify 131 goals that were extracted from the 23 privacy policies (6 pharmaceutical companies, 7 health insurance companies, and 10 online pharmacies)<sup>4</sup>. We now briefly discuss the heuristics used to classify the privacy policy goals extracted from these policies according to our privacy management framework.

<sup>4</sup> Additional information pertaining to this study is available at: <http://theprivacyplace.org/>

Classification of the health care privacy policy goals involves differentiating goals according to the five perspectives of the framework. Legal goals are classified by analyzing each goal and asking, “Does this goal have any legal implications?” Consider the goal G<sub>1</sub>: DISCLOSE collected PII when required by law; this goal clearly provides information about a legitimate legal constraint and is thus classified as a legal goal. Business goals are classified by asking: “Does this goal directly support the organization’s business objectives?” Consider the goal G<sub>2</sub>: SELL aggregate information; this goal directly reflects business opportunities presented by the sale of gathered information and is thus classified as a business goal. Technical goals are classified by asking: “Does this goal focus on domain specific implementation details?” Consider the goal G<sub>3</sub>: PROTECT order information using SSL encryption technology; this goal is classified as a technical goal because it clearly focuses on a technical solution for protecting user information. Contractual goals are classified by asking: “Does this goal focus on the relationship between a given organization and its business partners (e.g. third party affiliates or partners)?” Consider the goal G<sub>5</sub>: ALLOW affiliates to use PII for marketing and promotional purposes; this goal impacts the relationship between business partners and is thus classified as a contractual goal. Social goals are classified by asking: “Does this goal address the relationship between a given organization and consumers?” Consider the goal G<sub>4</sub>: ALLOW customer to modify/remove their PII; this goal offers the user an opportunity to manage their relationship with the organization and is thus classified as a social goal.

Our analysis of 23 privacy policies yielded 131 goals, each of which was easily classified according to each of the five perspectives. Additionally, there were 403 total indications (or occurrences) of the 131 goals. For example, the goal G<sub>4</sub>: ALLOW customer to modify/remove their PII had 16 indications in the 23 analyzed privacy policies. In other words, we found 16 occurrences of that particular goal within our 23 privacy policies. It appeared in two of the seven health insurance Web site privacy policies, ten of the ten drugstore Web site privacy policies and four of the six pharmaceutical company Web site privacy policies. Similarly, the goal G<sub>2</sub>: SELL aggregate information appeared in only one of the privacy policies; therefore, it had only one indication. It is important to note that we encountered no goals that overlapped classes. Table 1 provides an overview of the framework analysis and shows the number of indications for the five perspectives. These indication numbers are also broken down as either privacy protection goals or privacy obstacles.

## 4 Framework Perspectives

In Section 3.3, we described the process of allocating (or classifying) policy goals to each of the five framework perspectives. Perspective refers to the capacity to view things in light of their true relations or relative importance. The framework proposed in this paper seeks to aid privacy management officers maintain a holistic view of privacy within the context of their organizations in tandem with how those perspectives constrain and influence information practices. Privacy policy and privacy practices must thus be considered within a larger, more comprehensive framework that recognizes the role and influence of the five perspectives (legal, technical, business, social and contractual). This section discusses each of the framework perspectives within the context of our analysis of Internet health care privacy policies.

### 4.1 Legal Perspective

The framework’s legal perspective concerns privacy goals and/or privacy obstacles that conform to, or are permitted by law, or established rules. Privacy policies must comply with 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 HIPPA (Health Insurance Portability and Accountability Act)<sup>5</sup>. Since the law is the most obvious influencer in the privacy policy and privacy management arena, the legal perspective is designated as the framework’s outer layer since these laws ultimately constrain the privacy practices of the inner layers (see Figure 1).

---

<sup>5</sup> Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. 1320d to d-8 (West Supp. 1998).

In our case 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 two legal goals discovered, specifically, goal G<sub>1</sub>: DISCLOSE collected PII when required by law. Furthermore, only 12 of the 403 indications were classified under the legal perspective and these were classified as privacy obstacles in our previous study (Antón et al. 2002). We naively expected the legal goals to provide privacy protection and were stunned to realize that instead these were privacy obstacles. For example, G<sub>1</sub>: DISCLOSE PII for tax purposes does not, in any way, support privacy protection. We expect this perspective 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. This will be addressed in the next phase of our study.

**Table 1: Summary of Goal Perspectives Indications in Health Care Internet Privacy Policy Analysis**

Framework Perspective	Goal Class	Health Insurance	Online Pharmacies	Pharmaceutical Companies	TOTAL Indications	% vulnerable and protection indications
<b>LEGAL</b> total: 12 (3%)	Vulnerability Protection	4 0	7 0	1 0	12 0	7% 0%
<b>BUSINESS</b> total: 35 (9%)	Vulnerability Protection	0 6	8 15	3 3	11 24	6% 11%
<b>TECHNICAL</b> total: 91 (23%)	Vulnerability Protection	11 12	23 27	10 8	44 47	25% 21%
<b>SOCIAL</b> total: 186 (46%)	Vulnerability Protection	13 20	35 72	14 32	62 124	35% 54%
<b>CONTRACTUAL</b> total: 79 (20%)	Vulnerability Protection	8 6	29 23	9 4	46 33	26% 14%
<b>SUBTOTAL</b>	Vulnerability Protection	36 44	102 137	37 47	175 228	
<b>TOTAL</b>					403	

#### 4.2 Technical Perspective

An open network, such as the Internet, contains several access points that are potential targets for hackers to penetrate an organization. Security measures are, therefore, necessary in all organizational networks, and the goals addressing such measures belong to the technical perspective. IT practitioners need to focus on technical measures necessary to provide a secure IT environment that effectively protects consumer privacy. Such measures should support IT processes inside the organization, data transfer across the Internet and security features on user systems. Additionally, ethical viewpoints of the organization should be embedded in design, implementation and use phases of IT systems. Although the information being delivered is more important than the delivery vehicle, this perspective is important because security mechanisms are used to shield the information (in transit and in storage) from unauthorized users. Technical goals 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 valuable 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 stakeholders 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 (e.g. third parties and Web-based consumers).

In our analysis, twenty-two goals reflected this technical perspective. Ninety-one of the total observed goal indications (23%) were technical perspective goals with almost half of these being protection goals and half being goal obstacles. This balance was expected since technology is used to protect users while also supporting the organizational goals of increasing and maximizing profits.

### **4.3 Business Perspective**

The framework's business perspective concerns enterprise objectives and activities of those engaged in purchase or sale of commodities and/or other financial transactions. An organization's privacy policy is greatly influenced by its business objectives. 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. The framework's business perspective seeks to facilitate the process of evaluating these information practices as expressed in organizational privacy policies. Focusing on the business perspective allows privacy managers to consider the notion of general trust by exploring the privacy-safeguard administration and management.

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 and beliefs of an organization may be in direct conflict with the values and beliefs 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 e-commerce and online health care business context, values and beliefs are extremely relevant. In particular, these values and beliefs are commonly reflected in an organization's privacy policy. Privacy policies express organizational values and beliefs that relate to organizational success factors, as well as users' privacy concerns that are reflected directly through their thoughts and actions. 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. Some organizations try to obtain as much value as possible from consumer data. They are often ready to sell it 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.

Trust is an important element of privacy policy. Normally we build trust while in a social setting of face-to-face meetings. Engaging in business transactions on the Internet is a blind process so we 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 our study, the share of business goal indications was 9%. The weight of classification was on protection that reflects the business goals as a positive trust indicator. The actual requirements expressed in a privacy policy are business goals, but they have to go through a series of filters (e.g. legal, technical). Furthermore, business goals are motivated by the social norms and contractual norms of an organization.

### **4.4 Contractual Perspective**

The contractual perspective focuses on the binding agreements that form the basis for information exchange between an organization and its business partners or customers. Using modern telecommunications and computing technology organizations are able to easily share information regardless of the geographical distance. Information and knowledge can quickly spread between organizations due to business relationships and contractual obligations. Contractual networks can generate new information when participants combine elements together and this causes consumer vulnerability to increase.

Data and information exchange frequently occur between several organizations based on a set of reciprocity norms. These inter-organizational relationships often become very political as organizations become influenced by transactions and communications between them. Additionally, in their search for new ways to do business, some 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 IT-based activities are the primary internal functions concerning security, these are significantly important. The contractual perspective focuses on how information transfer and information use by external organizations affects consumer privacy. We will look at the relationship between organizations and how they cooperate.

There were 79 indications of goals addressing the contractual perspective. This results in 20% of the total goal indications from the 23 privacy policies. The majority of these contractual indications were also classified as privacy goal obstacles rather than privacy protection goals.

#### 4.5 Social Perspective

The framework's social perspective 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 social perspective, thus, reflects the relationship between the consumers (Web site users) 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 goals differ from contractual goals in that social goals 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 goal is indicated as a social goal

Forty-six percent of the 403 goal indications addressed the social perspective. Specifically, we discovered 186 indications of social perspective goals within the 23 privacy policies. These goals were primarily classified as privacy protection goals rather than privacy goal obstacles. This implies that the organizations in this study are aware of the importance of their relationships with users and try to support user needs to protect privacy.

## 5 SUMMARY

In closing, the framework presented in this paper is based upon five organizational perspectives that influence privacy policy and practices: legal, technical, business, contractual and social. The legal perspective concerns legislation that must be adhered to and which constrains the other four perspectives. The technical perspective offers tools and techniques that support, and restrict, the manipulation of consumer data. The business perspective reflects the fact that business objectives and practices often pass through legal and technical filters. The business entities involved in online business (users, organization and third parties) have goals that are motivated by social and contractual norms that further restrict the organization. These perspectives offer a foundation for reasoning about enterprise and Internet privacy policy and privacy management. We believe the framework, when employed to create a privacy policy will ensure that privacy managers and officers adopt a more holistic view of the organizations information practices. Our case study demonstrates that the framework also provides a useful basis for analyzing and comparing privacy policy content.

Kluge views health care information privacy as an important global issue due to the ease of international travel, communication and exchange that are IT-enabled (Kluge 1996). We believe that the foreseeable future will bring evolutionary improvements in technology. When some IT-services are offered to the public globally with information and communication technology, for example mobile and wireless technology, we need the ability to evaluate the privacy policy of IT-services and consider among the different cultures, laws, directives, vocabularies and other frames of reference. We have restricted our study in this paper to U.S. based Web sites and plan to continue the study with European based Web sites as part of our future work to enable us to compare practices between the U.S. and Europe.

## ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under ITR Grant #0113792 and The Fulbright Center. The authors wish to recognize Turun Kauppaseura Saatio, Emil Aaltosen Saatio, Ella and Georg Ehrnroothin Saatio, Liikesivistysrahasto, and Yrjo Jahnssonin Saatio. Additionally, the authors thank Carlos Jensen, Colin Potts and William Stufflebeam for discussions leading to the development of this framework.

## REFERENCES

- Antón, A.I. and Earp, J.B., "A Taxonomy for Web Site Privacy Requirements," NCSU Technical Report TR-2001-14, 18 December 2001.
- Antón, A.I., Earp, J.B. and Reese, A. "Analyzing Web Site Privacy Requirements Using a Privacy Goal Taxonomy," Submitted to 10<sup>th</sup> Anniversary IEEE Joint Requirements Engineering Conference (RE'02), February 2, 2002.
- Antón, A.I. "Goal-Based Requirements Analysis," 2nd IEEE Int'l Conf. on Requirements Engineering (ICRE '96), Colorado, pp. 136-144, 15-18 April 1996.
- Antón, A.I. and Potts, C. "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.
- Brannigan, V.M. and Beier, B.R. (1995). Patient Privacy in the Era of Medical Computer Networks: A New Paradigm for a New Technology. *Medinfo*, 8 Pt 1: 640-643.
- Davenport, T. and Prusak, L. *Working Knowledge. How Organizations Manage What They Know*. Harvard Business School

Press. Boston, Massachusetts, 1998.

FTC, *Privacy Online: A Report to Congress*, <http://www.ftc.gov/reports/privacy3/>, Federal Trade Commission, June 1998.

FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*. A Report to Congress. Federal Trade Commission, 2000.

FTC, Eli Lilly Settles FTC Charges Concerning Security Breach, FTC Press Release, <http://www.ftc.gov/opa/2002/01/elililly.htm>, 18 Jan. 2002.

Kluge, E.H.W. "Professional Ethics as Basic for Legal Control of Health Care Information", *International Journal of Bio-Medical Computing*, 43, pp. 33-37, 1996.

Memon, N. and P.W.Wong. "Protecting Digital Media Content," *Communications of the ACM*, August 1997, pp.92-100.

Rindfleisch, T.C. (1997), Privacy, Information Technology, and Health Care, *Communications of the ACM*, August 1997, pp 92-100.

Schneier.B, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, Second ed., New York: Wiley, 1996.

van Lamsweerde, A. "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.