Foundations and Trends® in
Human–Computer Interaction
Vol. 1, No. 1 (2007) 1–137

DOI: 10.1561/1100000004

End-User Privacy in Human–Computer Interaction

Giovanni Iachello[1] **and Jason Hong**[2]

[1] *Georgia Institute of Technology, USA, giac@cc.gatech.edu*
[2] *Carnegie Mellon University, USA, jasonh@cs.cmu.edu*

Abstract

The purpose of this article is twofold. First, we summarize research on the topic of privacy in Human–Computer Interaction (HCI), outlining current approaches, results, and trends. Practitioners and researchers can draw upon this review when working on topics related to privacy in the context of HCI and CSCW. The second purpose is that of charting future research trends and of pointing out areas of research that are timely but lagging. This work is based on a comprehensive analysis of published academic and industrial literature spanning three decades, and on the experience of both ourselves and of many of our colleagues.

1

Introduction

Privacy is emerging as a critical design element for interactive systems in areas as diverse as e-commerce [63], health care [287], office work [156], and personal communications. These systems face the same fundamental tension. On the one hand, personal information can be used to streamline interactions, facilitate communication, and improve services. On the other hand, this same information introduces risks, ranging from mere distractions to extreme threats.

Government reports [239, 283], essays [223], books [17, 93, 196, 303], and media coverage [252, 295, 312] testify on peoples' concerns regarding the potential for abuse and general unease over the lack of control over a variety of computer systems. Similarly, application developers worry that privacy concerns can impair the acceptance and adoption of their systems.

No end-to-end solutions exist to design privacy-respecting systems that cater to user concerns. Lessig provided a very high level framework for structuring the protection of individuals' privacy, which leverages four forces: laws, social norms, the market, and technical mechanisms [195]. However, the challenge is in turning these broad guidelines into actionable design solutions. Our thesis is that researchers in Human–Computer Interaction (HCI) and Computer-Supported Cooperative Work (CSCW) can greatly improve the protection of individual's personal information, because many of the threats and vulnerabilities associated with privacy originate from the interactions between the people using information systems, rather than the actual systems themselves.

Approaching the topic of privacy can be daunting for the HCI practitioner, because the research literature on privacy is dispersed across multiple communities, including computer networking, systems, HCI, requirements engineering, management information systems (MIS), marketing, jurisprudence, and the social sciences. Even within HCI, the privacy literature is fairly spread out. Furthermore, many IT professionals have common-sense notions about privacy that can turn out to be inaccurate.

Hence, the goal of this article is to provide a unified overview of privacy research in HCI, focusing specifically on issues related to the design and evaluation of end-user systems that have privacy implications. In Section 2, we present two philosophical outlooks on privacy that will help the practitioner frame research questions and design issues. We also show how privacy research has evolved in parallel with HCI over the past 30 years. Section 3 presents an overview of the research literature, structured along an ideal inquiry-build-evaluate development cycle. Finally, in Section 4, we outline key research challenges, where we think that HCI methods and research approaches can make a significant impact in furthering our knowledge about information privacy and personal data protection.

In the remainder of this section, we explain why we think privacy research is challenging and interesting for HCI, and map out relevant literature published in HCI conferences and journals, and in neighboring fields such as MIS and CSCW.

1.1 Why Should HCI Researchers Care About Privacy?

Human–computer interaction is uniquely suited to help design teams manage the challenges brought by the need of protecting privacy and personal information. First, HCI can help understand the many notions of privacy that people have. For example, Westin describes four states of privacy: solitude, intimacy, anonymity, and reserve [302]. Similarly, Murphy lists the following as expressions of privacy: “to be free from physical invasion of one’s home or person,” “the right to make certain personal and intimate decisions free from government interference,” “the right to prevent commercial publicity of one’s own name and image,” and “the control of information concerning an individual’s person” [212]. These perspectives represent different and sometimes conflicting worldviews on privacy. For example, while some scholars argue that privacy is a fundamental right, Moor claims that privacy is not a “core value” on par with life, security, and freedom, and asserts that privacy is just instrumental for protecting personal security [209].

Second, a concept of tradeoff is implicit in most discussions about privacy. In 1890, Warren and Brandeis pointed out that privacy should be limited by the public interest, a position that has been supported by a long history of court rulings and legal analysis [296]. Tradeoffs must also be made between competing interests in system design. For example, the developer of a retail web site may have security or business requirements that compete with the end-user privacy requirements, thus creating a tension that must be resolved through tradeoffs. Because HCI practitioners possess an holistic view of the interaction of the user with the technology, they are ideally positioned to optimally work through and solve these tradeoffs.

Third, privacy interacts with other social concerns, such as control, authority, appropriateness, and appearance. For example, while parents may view location-tracking phones as a way of ensuring safety and maintaining peace of mind, their children may perceive the same technology as smothering and an obstacle to establishing their identity. These relationships are compellingly exemplified in Goffman’s description of the behavior of individuals in small social groups [120]. For instance, closing one’s office door not only protects an individual’s privacy, but asserts his ability to do so and emphasizes the difference from other colleagues who do not own an individual office. Here, the discriminating application of HCI tools can vastly improve the accuracy and quality of the assumptions and requirements feeding into system design.

Fourth, privacy can be hard to rationalize. Multiple studies have demonstrated that there is a difference between privacy preferences and actual behavior [8, 39]. Many people are also unable to accurately evaluate low probability but high impact risks [256], especially related to events that may be far removed from the time and place of the initial cause [130]. For example, a hastily written blog entry or impulsive photograph on MySpace may cause unintentional embarrassment several years down the road. Furthermore, privacy is fraught with exceptions, due to contingent situations and historical context. The need for flexibility in these constructs is reflected by all the exceptions present in data protection legislation and by social science literature that describes privacy as a continuous interpersonal "boundary-definition process" rather than a static condition [17]. The use of modern "behavioral" inquiry techniques in HCI can help explicate these behaviors and exceptions.

Finally, it is often difficult to evaluate the effects of technology on privacy. There are few well-defined methods for anticipating what privacy features are necessary for a system to gain wide-scale adoption by consumers. Similarly, there is little guidance for measuring what level of privacy a system effectively offers or what its overall return on investment is. Like "usability" and "security," privacy is a holistic property of interactive systems, *which include the people using them.* An entire system may be ruined by a single poorly implemented component that leaks personal information, or a poor interface that users cannot understand.

In our opinion, HCI is uniquely suited to help design teams manage these challenges. HCI provides a rich set of tools that can be used to probe how people perceive privacy threats, understand how people share personal information with others, and evaluate how well a given system facilitates (or inhibits) desired privacy practices. Indeed, the bulk of this paper examines past work that has shed light on these issues of privacy.

As much as we have progressed our understanding of privacy within HCI in the last 30 years, we also recognize that there are major research challenges remaining. Hence, we close this article by identifying five "grand challenges" in HCI and privacy:

- — Developing standard privacy-enhancing interaction techniques.
- — Developing analysis techniques and survey tools.
- — Documenting the effectiveness of design tools, and creating a "privacy toolbox."
- — Furthering organizational support for managing personal data.
- — Developing a theory of technological acceptance, specifically related to privacy.

These are only few of the challenges facing the field. We believe that focusing research efforts on these issues will lead to bountiful, timely and relevant results that will positively affect all users of information technology.

1.2 Sources Used and Limitations of this Survey

In this survey paper, we primarily draw on the research literature in HCI, CSCW, and other branches of Computer Science. However, readers should be aware that there is a great deal of literature on privacy in the MIS, advertising and marketing, human factors, and legal communities.

The MIS community has focused primarily on corporate organizations, where privacy perceptions and preferences have a strong impact on the adoption of technologies by customers and on relationships between employees. The advertising and marketing communities have examined privacy issues in reference to privacy policies, and the effects that these have on consumers (e.g., work by Sheehan [257]).

The legal community has long focused on the implications of specific technologies on existing balances, such as court rulings and the constitutional *status quo*. We did not include legal literature in this article because much scholarly work in this area is difficult to use in practice during IT design. However, this work has some bearing on HCI and researchers may find some analyses inspiring, including articles on data protection [249], the relation between legislation and technology

[195], identity [171], data mining [311], and employee privacy [188]. As one specific example, Strahilevitz outlines a methodology for helping courts decide on whether an individual has a reasonable expectation of privacy based on the social networking literature [272]. As another example, Murphy discusses whether or not the default privacy rule should allow disclosure or protection of personal information [212].

Privacy research is closely intertwined with security research. However, we will not refer HCI work in the security field. Instead, we direct readers to the books *Security and Usability* [67] and *Multilateral Security in Communications* [210] for more information.

We also only tangentially mention IT management. Management is becoming increasingly important in connection to privacy, especially after the enactment of data protection legislation [178]. However, academia largely ignores these issues and industry does not publish on these topics because specialists perceive knowledge in this area as a strategic and confidential asset. Governments occasionally publish reports on privacy management. However, the reader should be aware that there is much unpublished knowledge in the privacy management field, especially in CSCW and e-commerce contexts.

This survey paper also focuses primarily on end-users who employ personal applications, such as those used in telecommunications and e-commerce. We only partially consider applications in workplaces. However, perceived control of information is one of the elements of acceptance models such as Venkatesh et al.'s extension [289] of the Technology Acceptance Model [74]. Kraut et al. discuss similar acceptance issues in a CSCW context [183], pointing out that in addition to usefulness, critical mass and social influences affect the adoption of novel technologies.

2

The Privacy Landscape

In this chapter, we introduce often-cited foundations of the privacy discourse. We then discuss two perspectives on privacy that provide useful characterizations of research and design efforts, perspectives that affect how we bring to bear the notions of law and architecture on the issue of privacy. These perspectives are (1) the grounding of privacy on principled views as opposed to on common interest, (2) the differences between informational self-determination and personal privacy. Finally, we provide a historical outlook on 30 years of privacy HCI research and on how privacy expectations co-evolved with technology.

2.1 Often-Cited Legal Foundations

In this section, we describe a set of legal resources often cited by privacy researchers. In our opinion, HCI researchers working in the field of privacy should be familiar with all these texts because they show how to approach many privacy issues from a social and legal standpoint, while uncovering areas where legislation may be lacking.

Many authors in the privacy literature cite a renowned 1890 *Harvard Law Review* article by Judges Warren and Brandeis entitled *The Right* *to Privacy* as a seminal work in the US legal tradition [296]. Warren and Brandeis explicitly argued that the right of individuals to "be let alone" was a distinct and unique right, claiming that individuals should be protected from unwarranted publications of any details of their personal life that they might want to keep confidential.[1] In this sense, this right to privacy relates to the modern concept of *informational self-determination*. It is interesting to note that Warren and Brandeis did not cite the US Constitution's Fourth Amendment,[2] which protects the property and dwelling of individuals from unwarranted search and seizure (and, by extension, their electronic property and communications). The Fourth Amendment is often cited by privacy advocates, especially in relation to surveillance technologies and to attempts to control cryptographic tools. The Fourth Amendment also underpins much privacy legislation in the United States, such as the Electronic Communications Privacy Act, or ECPA.[3] Constitutional guarantees of privacy also exist in other legal texts, for example the EU Convention on Human Rights [61, Article 8].

In the United States, case law provides more material for HCI practitioners. Famous cases involving the impact of new technologies on the privacy of individuals in the United States include Olmstead vs. United States (1928), which declared telephone wiretapping constitutional; Katz vs. United States (1967), again on telephone wiretapping and overturning Olmstead; Kyllo vs. United States (2001), on the use of advanced sensing technologies by police; and Barnicki vs. Vopper (2001) on the interception of over-the-air cell phone transmissions.

Regulatory entities such as the FTC, the FCC, and European Data Protection Authorities also publish rulings and reports with which HCI professionals working in the field of privacy should be familiar.

[1] Warren and Brandeis claimed that the right to privacy is unique because the object of privacy (e.g., personal writings) cannot be characterized as intellectual property nor as a property granting future profits.

[2] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, [. . .]."

[3] The ECPA regulates the recording of telecommunications and personal communications at the US Federal level, including wiretapping by government agencies. It generally outlaws any recording of which at least one party being recorded is not aware and requires various types of warrants for wiretapping or recording other telecommunication data for law enforcement purposes.

For example, the EU Article 29 Working Party has issued a series of rulings and expressed opinions on such topics as the impact of video surveillance, the use of biometric technologies, and the need for simplified privacy policies.

Finally, HCI researchers often cite legal resources such as the European Data Protection Directive of 1995 [79] and HIPAA, the US Health Insurance Portability and Accountability Act of 1999 [285]. Many of these data protection laws were inspired by the Fair Information Practices (discussed in more detail in Section 3.5.1), and impose a complex set of data management requirements and end-user rights. HCI practitioners should be aware that different jurisdictions use legislation differently to protect privacy, and that there is much more to privacy than the constitutional rights and laws described above.

2.2 Philosophical Perspectives on Privacy

Arguments about privacy often hinge on one's specific outlook, because designers' values and priorities influence how one thinks about and designs solutions [108]. In this section, we present alternative perspectives on privacy without advocating one particular view. The reader should instead refer to ethical principles suggested by professional organizations, such as the ACM or the IFIP [25, 41]. Still, we believe that an understanding of different perspectives is useful, because it provides a framework for designers to select the most appropriate approach for solving a specific problem.

2.2.1 Principled Views and Common Interests

The first perspective contrasts a principled view with a communitarian view. The *principled view* sees privacy as a fundamental right of humans. This view is supported by modern constitutions, for example the US 4th Amendment, and texts such as the European Convention on Human Rights [61]. In contrast, the *communitarian view* emphasizes the common interest, and espouses an utilitarian view of privacy where individual rights may be circumscribed to benefit the society at large [93]. For an example of how this dichotomy has been translated into a framework for assessing the privacy concerns brought about by ubiquitous computing technologies, see work by Terrel, Jacobs, and Abowd [159, 278].

The tension between principled approaches and utilitarian views is reflected in debates over the use of many technologies. For example, Etzioni discusses the merits and disadvantages of mandatory HIV testing and video surveillance. In the case of information and communication technologies, the contrast between these two views can be seen in the ongoing debate between civil liberties associations (e.g., the Electronic Frontier Foundation) and governments over strong encryption technologies and surveillance systems.

These contrasting views can also help explain differences in approaches in the privacy research community. For example, some privacy-enhancing technologies (PETs) have been developed more as a matter of principle than on solid commercial grounds. Some researchers in the privacy community argue that the mere existence of these PETs is more important for their impact on policy debate than their actual widespread use or even commercial viability. Reportedly, this is the reason why organizations such as the Electronic Frontier Foundation support some of these projects.

2.2.2 Data Protection and Personal Privacy

The second perspective contrasts data protection with personal privacy. *Data protection* (also known as informational self-determination) refers to the management of personally identifiable information, typically by governments or commercial entities. Here, the focus is on protecting such data by regulating how, when, and for what purpose data can be collected, used, and disclosed. The modern version of this concept stems from work by Alan Westin and others [302, 303], and came about because of concerns over how databases could be used to collect and search personal information [283].

Westin's work led to the creation of the influential Fair Information Practices (FIPS), which are a set of guidelines for personal information management. The FIPS include notions such as purpose specification, participation, and accountability (see Section 3.5.1). The FIPS have greatly influenced research on privacy, including standards like P3P [66], privacy policies on web sites, and data management policies [172]. More recently, the FIPS have been reinterpreted with reference to RFID systems [112] and ubiquitous computing [186].

In contrast, *personal privacy* describes how people manage their privacy with respect to other individuals, as opposed to large organizations. Drawing from Irwin Altman's research on how people manage personal space [17], Palen and Dourish argue that privacy is not simply a problem of setting rules and enforcing them, but rather an ongoing and organic "boundary definition process" in which disclosure and identity are fluidly negotiated [227]. The use of window blinds and doors to achieve varying levels of privacy or openness is an example of such boundary setting. Other scholars have made similar observations. Darrah et al. observed that people tend to devise strategies "to restrict their own accessibility to others while simultaneously seeking to maximize their ability to reach people" [73]. Westin argued that "Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication" [302].

Altman's work is in part inspired by Goffman's work on social and interpersonal relations in small groups [119, 120]. One of Goffman's key insights is that we project different personas to different people in different situations. For example, a doctor might present a professional persona while working in the hospital, but might be far more casual and open with close friends and family. The problem with respect to the design of interactive systems is that these roles cannot always be easily captured or algorithmically modeled.

Personal privacy appears to be a better model for explaining peoples' use of IT in cases where the information requiring protection is not well defined, such as managing one's availability to being interrupted or minute interpersonal communication. Here, the choice of whether or not to disclose personal information to others is highly situational depending on the social and historical context of the people involved. An example of this is whether or not to disclose one's location when on-the-go using cell phones or other kinds of "friend finders" [158]. Current research suggests that these kinds of situations tend to be difficult to model using rigid privacy policies that are typical of data protection guidelines [192].

In summary, data protection focuses on the relationship between individual citizens and large organizations. To use a blunt expression, the power of knowledge here lies in *quantity*. In contrast, personal privacy focuses more on interpersonal relationships and tight social circles, where the concern is about *intimacy*.

This distinction is not just academic, but has direct consequences on design. Modeling privacy according to data protection guidelines will likely result in refined access control and usage policies for personal information. This is appropriate for many IT applications today, ranging from healthcare to e-commerce. Typical design tools based on the data protection viewpoint include privacy policies on web sites, consent checkboxes, certification programs (such as TRUSTe), and regulations that increase the trust of consumers toward organizations.

For applications that manage access to one's physical space or attention or interpersonal communication (e.g., chat, email, and social networking sites, as well as some location-enhanced applications such as person finders), a data protection outlook may result in a cumbersome design. For example, imagine highly detailed policies to limit when others can send instant messages to you. Instead, IM clients provide a refined moment-by-moment control of availability through "away" features and plausible deniability. For applications affecting personal privacy, negotiation needs to be dialectic and continuous, making it easy for people to project a desired persona, depending on social context, pressures, and expectations of appropriate conduct.

How should these different views of privacy be reconciled? Our best answer to this question is that they should not be. Each approach to privacy has produced a wealth of tools, including analytic instruments, design guidelines, legislation, and social expectations. Furthermore, many applications see both aspects at work at the same time. For example, a social networking web site has to apply a data protection perspective to protect the data they are collecting from individuals, a personal privacy perspective to let individuals project a desired image of themselves, and a data protection perspective again to prevent users from crawling and data mining their web site.

2.3 An Historic Perspective on Privacy

Privacy is not a static target: changes in technology, in our understanding of the specific social uses of such technologies, and in social expectations have led to shifts in the focus of privacy research in HCI. In this section, we discuss changes in the expectation of privacy over the past three decades and summarize the consequences of these changes on HCI practice.

2.3.1 Changes in Expectations of Privacy

While the basic structures of social relations — for example, power relations and the presentation of self — have remained relatively stable with technical evolution [119], there have been large shifts in perceptions and expectations of privacy. These shifts can be seen in the gradual adoption of telecommunication technologies, electronic payment systems, and surveillance systems, notwithstanding initial privacy worries.

There are two noteworthy aspects on how privacy expectations have changed. The first is that social practice and expectations co-evolve with technical development, making it difficult to establish causal effects between the two. The second aspect is that privacy expectations evolve along multi-dimensional lines, and the same technology can have opposite effects on different types of privacy.

Social practice and technology co-evolve. For example, the introduction of digital cameras, or location technology in cell phones, happened alongside the gradual introduction of legislation [78, 284, 286] and the emergence of a social etiquette regulating their use. Legislation often follows technical development, but in some cases it preempts technical development. For example, digital signature legislation in some European countries was enacted well before the technology was fully developed, which may have in fact slowed down adoption by negatively affecting its usability [1].

It is often difficult to tease cause and effect apart: whether social practices and expectations drive the development of technology or vice-versa. Some observers have noted that the relationship between social constructs and technology is better described as *co-evolution*. Latour talks of “socio-technological hybrids,” undividable structures encompassing technology as well as culture — norms, social practices and perceptions [189]. Latour claims that these hybrids should be studied as a whole. This viewpoint is reflected by HCI researchers, including the proponents of participatory design [88, 251] and researchers of social computing [81]. Iachello et al. even go as far as claiming that in the domain of privacy, adoption patterns should be "designed" as part of the application and can be influenced to maximize the chances of successful acceptance [154].

The reader should note that in some cases, technologies that affect privacy are developed without much public debate. For example, Geographic Information Systems (GIS) classify geographic units based on census, credit, and consumer information. Curry and Philips note that GIS had a strong impact on the concepts of community and individual, but were introduced almost silently, over the course of several decades, by a combination of government action, developments in IT, and private enterprises, without spurring much public debate [72].

Understanding these changes is not a straightforward task, because technical development often has contradictory effects on social practice. The same artifact may produce apparently opposite consequences in terms of privacy, strengthening some aspect of privacy and reducing others. For example, cell phones both increase social connectedness, by enabling distant friends and acquaintances to talk more often and in a less scheduled way than previously possible, but also raise barriers between physically co-present individuals, creating "bubbles" of private space in very public and crowded spaces such as a train compartment [23].

From this standpoint, privacy-sensitive IT design becomes an exercise of systematically reconciling potentially conflicting effects of new devices and services. For example, interruption management systems based on sensing networks (such as those prototyped by Nagel et al. [214]) aim at increasing personal and environmental privacy by reducing unwanted phone calls, but can affect information privacy due to the collection of additional information through activity sensors. We highlight this issue of how expectations of privacy change over time as an ongoing research challenge in Section 4.5.

2.3.2 Changes in Privacy Methodologies

The discourses on HCI and on privacy in IT share a similar history over the past 40 years. Reflections on the implications of IT on privacy surged in the late 1960's with the proposal of a National Data Center in the United States [84] and culminated with the publication of the 1973 report *Records, Computers and the Rights of Citizens* [283] which introduced the Fair Information Practices. By the early 1970s, the accumulation of large amounts of personal data had prompted several industrialized countries to enact laws regulating the collection, use, and disclosure of personal information.

The FIPS reflect the top-down and systems approach typical of IT at the time. Systems were relatively few, carefully planned, developed for a specific purpose, centrally managed, and their use was not discretionary. The terminology used to describe privacy reflects this perspective as well. *Data subjects* were protected through *data protection* mechanisms, which were centrally administered and verified by a *data controller* or *data owner* (the organization managing the data). Trust originated in the government and in the accountability of data owners. HCI in the 1970s also reflected carefully planned, structured process modeling of non-discretionary applications [131]. Computer-related work tasks were modeled and evaluated to improve performance, usability, and effectiveness using techniques such as GOMS [126].

This picture began to change with advances in personal computing. Discretionary use became the predominant mode for many applications, even in office settings, and HCI started to concentrate more on ease-of-use, learning curves, and pleasurable interaction. Users enjoyed increasing discretion of what applications and services to employ. At the same time, the collection of personal data expanded with advances in storage and processing power, making trust a fundamental component in the provisioning of IT services. This increased choice and shift of approaches is reflected in data protection legislation in the 1980s, where the original concepts of *use limitation* gives way to the more far-reaching concept of *Informational Self-Determination* [116].

Finally, the 1990s saw the emergence of the Internet, which enabled new kinds of applications and forms of communication. Regulators and industry started developing more flexible and comprehensive legislation to support the greatly increased amounts of personal information that was being shared and used. Privacy research followed these changes, acknowledging the use of IT for communication purposes and the increasing fluidity of personal information collected and used by individuals, businesses, and governments. The development of privacy-enhancing technologies like machine-readable privacy policies [66], of concepts such as Multilateral Security [241], and of technology supporting anonymous transactions (e.g., mail encryption tools, mix networks, anonymizing web services) are manifestations of the complexity of the IT landscape.

At the same time, HCI research and practices began to focus on the use of IT to enable interpersonal communications and support social and work groups, first in small environments such as offices, later in society at large. Example domains studied by HCI researchers at this time include remote collaboration, telecommunications, and organizations. Following these developments, interpersonal relations became an important domain of the privacy discourse, and research started to focus on interpersonal privacy within office environments [114, 211] and in everyday interactions and communications (e.g., instant messaging, email).

Today, the combination of wireless networking, sensors, and computing devices of all form factors has spurred the development of new kinds of mobile and ubiquitous computing applications. Many of these new applications operate in non-traditional settings, such as the home or groups of friends, which lead to new challenges for HCI and privacy [186, 262]. For example, the implicit nature of interaction with these systems requires developers to re-think both Norman's seven steps of interaction [222] and established tenets of privacy such as informed consent [5]. Furthermore, the type, quantity and quality of information collected from ubicomp environments significantly heighten risks of misuse.

This brief historical review should have convinced the reader that privacy is a very dynamic construct, and that design for privacy is a function of social and technological contexts, which vary over time. Against this backdrop, we next survey the research landscape of privacy in HCI.

3

Understanding, Building and Evaluating Privacy in Interactive Systems

In this chapter, we survey HCI privacy literature, organized according to threads of research on specific topics, such as mobile computing or identity management. Privacy research in the HCI field has seen a surge starting in the early 1990's and is now booming. The increased interest in privacy within HCI is also testified by countless workshops at HCI conferences, and the recent creation of conferences like SOUPS (Symposium on Usable Privacy and Security).

Figure 3.1 depicts our view of the evolution of HCI privacy research between 1970 and 2006. Each line represents a particular subfield, defined as a timeline of related work (e.g., location-enhanced technologies privacy). Beneath each line, we provide a sample of salient studies (which are referenced in the bibliography). Note that the intent is not to provide an exhaustive listing of references, but to illustrate with select references the scope of each line of research.

The figure clearly shows the dichotomy between personal privacy research and data protection, described above in Section 2.2.2. The picture also shows shaded regions (see Section 2.3):

— the non-discretionary era of centralized personal data management (1960–1980);

— the period of informational self-determination (1980–2000);
— the more recent developments toward implicit interaction and behavioral analysis of users with respect to privacy concerns (2000 to present).

In the following sections, we describe the main research efforts and results in the subfields of Figure 3.1. The material is organized according to an ideal application development cycle, from understanding user needs, to designing the application, to evaluating it.

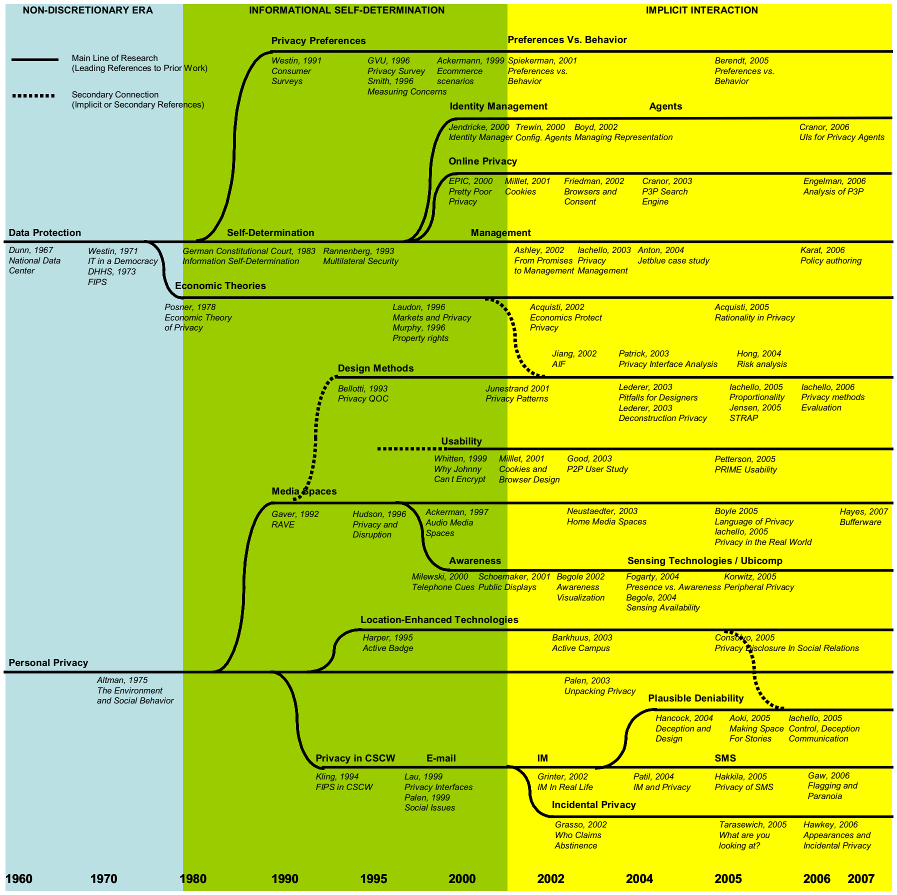

NON-DISCRETIONARY ERA
INFORMATIONAL SELF-DETERMINATION
IMPLICIT INTERACTION
Main Line of Research (Leading References to Prior Work)
Secondary Connection (Implicit or Secondary References)
Privacy Preferences
Westin, 1991 Consumer Surveys
GVU, 1996 Privacy Survey
Smith, 1996 Measuring Concerns
Ackermann, 1999 Ecommerce scenarios
Preferences Vs. Behavior
Spiekerman, 2001 Preferences vs. Behavior
Berendt, 2005 Preferences vs. Behavior
Identity Management
Agents
Jendricke, 2000 Identity Manager
Trewin, 2000 Config. Agents
Boyd, 2002 Managing Representation
Cranor, 2006 UIs for Privacy Agents
Online Privacy
EPIC, 2000 Pretty Poor Privacy
Milllet, 2001 Cookies
Friedman, 2002 Browsers and Consent
Cranor, 2003 P3P Search Engine
Engelman, 2006 Analysis of P3P
Data Protection
Self-Determination
Management
Dunn, 1967 National Data Center
Westin, 1971 IT in a Democracy
DHHS, 1973 FIPS
German Constitutional Court, 1983 Information Self-Determination
Rannenberg, 1993 Multilateral Security
Ashley, 2002 From Promises to Management
Iachello, 2003 Privacy Management
Anton, 2004 Jetblue case study
Karat, 2006 Policy authoring
Economic Theories
Posner, 1978 Economic Theory of Privacy
Laudon, 1996 Markets and Privacy
Murphy, 1996 Property rights
Acquisti, 2002 Economics Protect Privacy
Acquisti, 2005 Rationality in Privacy
Jiang, 2002 AIF
Patrick, 2003 Privacy Interface Analysis
Hong, 2004 Risk analysis
Design Methods
Bellotti, 1993 Privacy QOC
Junestrand 2001 Privacy Patterns
Lederer, 2003 Pitfalls for Designers
Lederer, 2003 Deconstruction Privacy
Iachello, 2005 Proportionality
Jensen, 2005 STRAP
Iachello, 2006 Privacy methods Evaluation
Usability
Whitten, 1999 Why Johnny Can t Encrypt
Milllet, 2001 Cookies and Browser Design
Good, 2003 P2P User Study
Petterson, 2005 PRIME Usability
Media Spaces
Gaver, 1992 RAVE
Hudson, 1996 Privacy and Disruption
Ackerman, 1997 Audio Media Spaces
Neustaedter, 2003 Home Media Spaces
Boyle 2005 Language of Privacy
Iachello, 2005 Privacy in the Real World
Hayes, 2007 Bufferware
Awareness
Sensing Technologies / Ubicomp
Milewski, 2000 Telephone Cues
Schoemaker, 2001 Public Displays
Begole 2002 Awareness Visualization
Fogarty, 2004 Presence vs. Awareness
Begole, 2004 Sensing Availability
Korwitz, 2005 Peripheral Privacy
Location-Enhanced Technologies
Harper, 1995 Active Badge
Barkhuus, 2003 Active Campus
Consolvo, 2005 Privacy Disclosure In Social Relations
Personal Privacy
Altman, 1975 The Environment and Social Behavior
Palen, 2003 Unpacking Privacy
Plausible Deniability
Hancock, 2004 Deception and Design
Aoki, 2005 Making Space For Stories
Iachello, 2005 Control, Deception Communication
Privacy in CSCW
E-mail
IM
SMS
Kling, 1994 FIPS in CSCW
Lau, 1999 Privacy Interfaces
Palen, 1999 Social Issues
Grinter, 2002 IM In Real Life
Patil, 2004 IM and Privacy
Hakkila, 2005 Privacy of SMS
Gaw, 2006 Flagging and Paranoia
Incidental Privacy
Grasso, 2002 Who Claims Abstinence
Tarasewich, 2005 What are you looking at?
Hawkey, 2006 Appearances and Incidental Privacy
1960
1970
1980
1990
1995
2000
2002
2004
2005
2006
2007

Fig. 3.1 Timeline of HCI privacy research.

3.1 Understanding Users' Privacy Preferences

We start by describing work on understanding the privacy preferences of individuals. As noted above, privacy preferences are determined by social context and are sometimes difficult to articulate. For example, the need for plausible deniability is evident in social relations [77], but participants of a survey may not admit it or be consciously aware of certain dynamics that are ingrained in one's daily behavior. Consequently, privacy preferences and concerns can be difficult to generalize and should be probed with reference to a specific circumstance. One implication is that it can be misleading to take privacy preferences from one domain (e.g., attitudes toward the use of loyalty cards or internet shopping) and extrapolate them to another domain (e.g., social relations such as family and colleagues).

Notwithstanding these difficulties, a wide array of techniques has been developed to gather data about users' preferences and attitudes. These techniques include both quantitative tools, such as surveys to probe mass-market applications, and qualitative techniques to probe personal privacy dynamics. Table 3.1 provides an overview of the research space, with a sampling of the most used techniques and a few representative studies for each, with an indication of their scope, advantages and limitations. We first show how these techniques have been used in several application domains. In Section 3.2, we discuss the drawbacks and advantages of specific techniques, specifically in relation to privacy. In Section 4.3, we argue that there is still a great need for improving these techniques.

3.1.1 Data Protection and Privacy Preferences

The development of data collection practices during the 1970s and 1980s led governments to enact data protection legislation. At the same time, a number of studies were conducted to probe public opinion regarding these practices. Many of these studies were commissioned or conducted by the government, large IT companies, or research institutions. In the United States, a well-known series of surveys was developed by the Pew Research Center, a non profit organization that provides

Table 3.1 Summary of techniques for understanding users' privacy preferences, with example studies.

Technique	**Scope**	**Data protection/ personal privacy**	**Principled/ communitarian**	**Sample size**	**Advantages**	**Disadvantages**
Surveys						
Westin	Segmentation	Data protection	Principled	1000–10000	Simple Statistically significant	Probes opinions Only superficial
GVU	General preferences	Data protection	Neutral	10000	Historic sequence of studies	
Smith et al.	Data protection in organizations	Data protection	Neutral	<1000	Validated	Not adequate for new technologies
Scenario-based surveys						
Spiekermann	Control in ubicomp	Data protection	Communitarian	128	Validated Realism Control	Bias Probes opinions only
Olson et al.	Two-phased (identify items, then probe prefs)	Personal	Neutral	30–80	Efficient use of participants	Bias Probes opinions only
Hawkey and Inkpen	Incidental privacy	Personal	Principled	155		Bias Probes opinions only

Table 3.1 (*Continued*).

Technique	**Scope**	**Data protection/ personal privacy**	**Principled/ communitarian**	**Sample sizes**	**Advantages**	**Disadvantages**
ESM/Simulations						
Consolvo et al.	Location privacy	Personal	Principled	16	Realism Immediacy	Implausibility Cost Intrusiveness
Ammenwerth et al.	Mobile computing	Personal	Neutral	31	Expert feedback Realism immediacy	Extensive training requires experts Cost Intrusiveness
Iachello et al.	Mobile computing	Personal	Communitarian	41	Realism Immediacy	Cost Intrusiveness
Focus groups						
Kaasinen	Relation of user with Telecoms	Data protection	Neutral	13 groups, 3–7 people each	Rich data Efficient	Requires experts Crosstalk
Hayes	School-based surveillance	Personal	Neutral	4 groups, 4–5 people each	Rich data Efficient	Requires experts Crosstalk
Interviews						
March et al.	Mobile phones	Personal	Neutral	10–20	Rich data probes sensitive topics	Cost
Melenhorst	Ubiquitous computing	Personal	Neutral	44	Rich analysis	Requires demonstration cost

Table 3.1 (*Continued*).

Technique	**Scope**	**Data protection/ personal privacy**	**Principled/ communitarian**	**Sample sizes**	**Advantages**	**Disadvantages**
Experiments						
Kindberg	Mobile payment systems trust	Personal	Neutral	24	Scientifically Sound Control	Cost Difficult to reproduce realistic situations
Jensen	e-commerce	Data protection	Neutral	175	Statistical significance Control	Cost Difficult to reproduce realistic situations
Case studies						
Anton	Airlines and government	Data protection	Principled	2	Reference to real systems	Insider access or extensive public literature search Anecdotal
Esslinger	PKI in banks	Personal	Neutral	1	Reference to real systems	Insider access or extensive public literature search Anecdotal
Participatory design (Muller et al.)	*Project management groupware system*	*Personal*	*Principled*	1	*Buy-in of users* *Rich analysis*	*Costly embedded in development*

information on the attitudes and trends shaping American public opinion [232].

One of the most cited series of surveys was conducted by Privacy & American Business [238], a research consultancy founded by Alan Westin (who also worked on the initial version of the FIPS). Westin's surveys have been used to segment people into three categories based on their privacy preferences toward commercial entities [304]. *Fundamentalists* are those individuals who are most concerned about privacy, believe that personal information is not handled securely and responsibly by commercial organizations, and consider existing legislative protection to be insufficient. *Unconcerned* individuals are not worried about the handling of their personal data and believe that sufficient safeguards are in place. *Pragmatists*, which are the majority of the sampled population, lie somewhere in the middle. They acknowledge risks to personal information but believe that sufficient safeguards are in place.

Temporal trends over the past ten years show that the distributions in the three categories vary over time [301], and in general, the percentages hover around 15%–25% fundamentalists, 15%–25% unconcerned, and 40%–60% pragmatists. Similar figures are reported by the Eurobarometer survey in the EU [98]. This distribution has also been observed in a scenario-based survey by Ackerman et al. [3] and in a controlled experiment [165].

This kind of segmentation allows service providers to devise service improvements or marketing strategies. For example, both Ackerman et al. and Jensen et al. have attempted to characterize individual behavior on retail web sites based on Westin's privacy classifications. Specifically, Jensen et al. found that while the purchasing decisions of those classified as pragmatists and unconcerned were affected by the presence of trust marks and privacy policies on web sites, fundamentalists' decisions were not [165].

Culnan and Armstrong's scenario-based survey also examined the propensity of people to disclose personal information in ecommerce settings [71]. The repeated-measures survey was administered by phone to 1000 individuals using two scenarios that involved the collection of personal information. In the first scenario, the researchers did not indicate that fair information practices would be employed, while in the second, they specified that the data collector would apply control and notification measures. In the first condition, people with a high degree of concern for privacy would disclose information less often than the others, while in the second condition, there was no difference. Interestingly, these results on the effect of privacy assurances differ from Jensen et al.'s conclusions.

While the privacy segmentation model is stable and identifies similar trends in different countries, it is much harder to associate a particular demographic to privacy preferences. Westin only found weak correlations between gender and concern [305]. Ackerman did not find any correlation [3]. The Eurobarometer survey showed that differences in privacy perceptions are attributable to different national contexts rather than demographics, presumably influenced by local legislative situation and media coverage [98].

Westin's survey has been employed to classify participants of experimental studies, to support the interpretation of results. However, the segmentation should be interpreted carefully, for two reasons. First, the Westin classification only probes opinions on the use of personal information by commercial entities, and can thus be described as examining people's attitudes toward data protection. It would be misleading to infer that views on data protection correspond to views on personal privacy with family, friends, and co-workers. In fact, Consolvo et al. found that there was no strong correlation in how participants responded to Westin's survey and how willing they were to disclose their current location to others with a "person finder" device [59].

Second, Kumaraguru and Cranor point out that the questions in the Westin surveys have changed over the years, based on the goals of the commercial entities commissioning the studies [184]. Thus, it is not immediately clear how well the results of past surveys can be combined with more recent surveys to establish trends.

Smith et al. developed a privacy attitudes questionnaire that is more elaborate than the Westin segmentation survey [263]. Like Westin's, Smith et al.'s questionnaire assesses concerns about privacy in data protection settings, and its validation procedure has been accurately documented. Based on an analysis of the responses of a large sample set, Smith et al. identified four subscales that constitute overall privacy concerns:

- concerns about collection of personal information,
- processing errors,
- further use of personal data (control), and
- improper access to the information.

The advantage of this questionnaire is that it decomposes privacy concerns in meaningful subscales (thus, providing more information than Westin's survey). However, this tool does not take into account new technologies such as the Internet and ubiquitous computing, nor does it consider issues of personal privacy. Smith et al.'s survey would thus require additions to be useful in these new research areas.

3.1.2 Privacy on the World Wide Web, Privacy and E-commerce

In the mid 1990's, privacy and security concerns were considered to be significant limiting factors to the development of e-commerce over the World Wide Web. For this reason, several surveys were conducted to assess privacy preferences of web users.

One such survey was Georgia Tech's World Wide Web User Survey, which was executed ten times between 1994 and 1998 [134]. The Fifth GVU survey (April 1996) asked three general questions about privacy notices and information. Over the following years, the range of questions about privacy and security grew, with the last survey containing 37 detailed questions on topics ranging from reporting security breaches to clearinghouse organizations, to children's online privacy. Results of the Tenth GVU survey (October 1998) show that the majority of surveyed internet users were very concerned about privacy and security in e-commerce, and that most favored the availability of FIPS-inspired data protection mechanisms such as collection notification and disclosure control. Participants in the GVU surveys were also grouped in three geographic regions (USA, Europe, and the rest of the world), but responses were similar across geographical areas.

The 1999 IBM Multi-National Consumer Privacy Study also probed consumers' perceptions across three large industrialized economies: the United States, the United Kingdom, and Germany [138]. IBM's survey is interesting because in a joint project, the manufacturer also surveyed executives in "high privacy risk" industries, including the health care, financial services, insurance, and retail industries. This survey showed that executives generally underestimated consumers' privacy concerns. The survey also indicated that more tech-savvy and educated respondents were more aware and more concerned about potential privacy violations online. Finally, respondents indicated the desire for notification mechanisms and an overall concern for privacy.

Subsequent research has however shown that privacy notices only partially assuage user concerns; well-known and reputable brands remain the most effective communication tools for this purpose. In 2003, Baumer et al. surveyed 415 individuals via email, probing their likelihood of disclosing information on e-commerce web sites as a function of the availability of privacy seals, privacy notices, and of the demographics of the respondents [31]. They found that respondents were more willing to reveal personal information in several categories to well-known web sites as compared to less well-known web sites. The presence of privacy policies and privacy seals only provided a marginal benefit, possibly due to skepticism regarding compliance. Baumer et al. argue that it is important to situate privacy questions with sufficient context to elicit reasonably accurate answers. Baumer et al.'s survey included a scenario before the actual questions to help situate the responses rather than leaving the decision context to the imagination of the user.

Since the late 1990's, many of the best practices indicated by these surveys have been widely adopted by e-commerce operators. However, IT manufacturers, such as IBM and Microsoft, still claim that privacy concerns are limiting the growth of online business, especially after several high-profile scandals [155, 205]. These manufacturers advocate stronger and uniform privacy protection legislation in countries that lack it, such as the United States.

3.1.3 Instant Messaging, Environmental Privacy, and Personal Availability

One aspect of online personal privacy relates to one's availability to communicate with others. New communication media alter the way individuals offer themselves to communication, based on the affordances of the medium. Two such media that have enjoyed widespread adoption in recent years are SMS and Instant Messaging (IM).

Patil and Kobsa interviewed seven participants on the privacy issues involved in IM [228]. Häkkilä and Chatfield surveyed people in two different locales (Finland and Australia) about SMS messaging practices and privacy expectations of the medium [135]. In both studies, the interviewees were very familiar with the domain being probed and were able to reflect on their behaviors and expectations, thus making them "expert informants." Results showed that the mobile device was perceived as a "private object" and that a strong etiquette protecting the confidentiality of voice and especially text communication existed within the social group (e.g., interviewees would not pick up others' phone calls, and expected the recipient of their text messages to preserve confidentiality). Häkkilä and Chatfield note that the selection of communication medium (SMS over voice) was influenced by confidentiality considerations. For example, SMS was considered more discreet than voice.

Grinter and Palen also studied teens' use of IM and SMS [127]. Like Häkkilä and Chatfield, Grinter and Palen found that the selection of the communication medium was based on privacy considerations (e.g., leaving no written trace) as well as convenience and availability. Specifically, Grinter and Palen showed how interviewees used the different features of IM to control access to themselves. At the same time, IM allowed users to keep a connection with their social group and to carve a private space in the household where they were unlikely to be overheard [158]. Grinter and Palen asked questions about privacy as part of a broad interview about usage patterns and social context, which we believe is conductive to balanced and realistic results. Grinter and Palen noticed that different members of an outwardly "homogeneous" demographic — teens — report very different behaviors in terms of privacy, which warns against standard "common sense" assumptions about privacy expectations and preferences. A similar observation was made by Iachello et al. [153] in relation to inter-family use of mobile person finders.

Privacy also emerged as a fundamental component in two ethnographic studies of teens' use of SMS, by Ito and Ling, respectively, [158, 197]. While these studies were not specifically designed to probe privacy, they exposed the relationship between privacy, group communication, accessibility, and familial power structures. Similar to Grinter and Palen, both Ito and Ling reported that the unobtrusive qualities of text messaging allowed teenagers to be connected with their social milieu even in situations where an open phone conversation would be inappropriate, such as a family dinner. They also discovered that environmental privacy (e.g., not interrupting or disturbing the physical environment) is an important aspect of communications for these teens.

The issues of environmental privacy and availability to communication can be extended to the sharing of other types of personal information with immediate relations. For example, Olson et al. probed information sharing practices in interpersonal settings [224]. They surveyed the propensity to share information such as availability to communication, contact information, and personal communication preferences with other people. Olson et al. identified clusters, based on the *type* of information respondents would share and the *recipient* of the information (i.e., family and friends, close colleagues, remote colleagues, and others).

Expectedly, Olson et al.'s study showed that individuals would share more sensitive information with closer acquaintances. It should be noted that Olson et al.'s study design was hypothetical. In a study using Experience Sampling, Consolvo et al. showed that disclosure of location information is heavily influenced by additional factors, including the purpose of the disclosure [59]. These differences suggest that personal privacy dynamics should be investigated with studies that closely simulate the experience of the users, rather than on a hypothetical basis.

3.1.4 Incidental Information Privacy

A common problem encountered when several individuals are viewing the same computer screen is that potentially private information, such as bookmarks or financial information, may be accidentally disclosed.

These accidental disclosures can happen, for example, when projecting onto a shared display or when a bystander happens to see someone else's screen (i.e., "shoulder surfing").

In a scenario-based survey, Hawkey and Inkpen confirmed that incidental eavesdropping is a concern for a majority of the surveyed participants [139]. Incidental eavesdropping relates to information that can be glanced from casually viewing the screen of a user or overhearing a conversation. Hawkey and Inkpen also investigated what kinds of information individuals may be comfortable having others see, specifically focusing on web browsers, past search engine queries, and browser bookmarks. They showed that the comfort level of the user in displaying personal information in the presence of onlookers is impacted not just by the sensitivity of the information being displayed, and by the identity of the viewer (e.g., spouse, friend/relative, work colleague), but also by the amount of control on the input devices (mouse, keyboard) that the onlooker has.

Managing incidental information disclosures is an example of the interpersonal boundary definition process described by Palen and Dourish [227]. Drawing from this approach, Grinter et al. [82] analyzed everyday security and privacy practices in an organizational setting, examining the problem of incidental privacy with respect to its *physical* and *informational* aspects. Through interviews, Grinter et al. observed that their interviewees employed subtle practices to achieve privacy and security goals, such as positioning a computer screen such that visitors in an office could not see it, or stacking papers according to a secret rationale.

The increasing use of IT in mobile and casual situations suggests that the potential for incidental information privacy breaches is likely to become more relevant in the future. It is likely that an increasing amount of research in HCI will focus on privacy with respect to incidental information, shared displays, and related topics.

3.1.5 Media Spaces

We next examine privacy preferences in the context of media spaces, which are physical spaces enhanced with multimedia communication or recording technologies such as videoconferencing and always-on multimedia links between remote locations. Privacy concerns were recognized early on in this domain. For example, Root discusses the design of Cruiser, a multimedia communication tool developed at Bell Research in the late 1980's [246]. Through observational research in office environments, Root noted that the activity of observing other people is typically symmetric, meaning that it is not possible to observe others without being seen. This principle was applied to the design of the Cruiser system. In addition, a *busy* feature was added to the design, allowing users to block communication at will [104].

Jancke et al. also studied the social effects of a multimedia communication system linking public spaces together [161]. In their work, Jancke et al. noted that symmetry and the ability to opt out were important design components of a privacy-respecting system.

Subsequent research, however, has showed that other concerns and design features are needed for successful implementations of media spaces. In a preliminary study of the organizational impact of a multimedia recording technology in special education classrooms, Hayes and Abowd led focus groups with professionals who would experience both the benefits and the potential downsides of the technology. Hayes and Abowd discovered that in addition to control, *purposefulness* was a fundamental aspect of the privacy balance of their design [140]. That is, users accepted potential privacy risks if they perceived the application to provide value either to them or to some other stakeholder.

We believe that during the development of novel technologies, such as media spaces, sensing systems, or location technologies, it is important to emphasize the *value proposition* of the technology. Users can thus express their privacy concerns and preferences with reference to the actual needs that are satisfied by the technology.

3.1.6 Ubiquitous Computing, Sensors, and RFID

One way of conveying the value proposition of a technology is to show a working example to the intended users. This may be problematic for technologies that are still at the conceptual stage, as is the case with many ubiquitous computing applications. Spiekermann proposed and partially validated a survey to probe privacy attitudes toward ubiquitous computing technologies [266]. She presented a short video demonstrating an application of RFID technology to participants, who then responded to a privacy survey. The video scenario provided people with an experience of how the application would work without actually having to build it.

Spiekermann's survey included questions on control, choice, and ease-of-use. Analysis identified three main concerns from respondents, namely concerns about further use of collected data, perceived helplessness, and ease-of-use of the technology. In particular, participants were concerned over a loss of control over the technology and uncertainties regarding the technology's utility and effective operation.

More realistic demonstrations may help users imagine the everyday operation of a new technology. Melenhorst et al. combined live demonstrations of sensing technologies with interviews probing the perceived usefulness and privacy concerns of the intended users [204]. Elderly interviewees were shown several home-based ubiquitous computing applications, for example, an activity monitor that distant relatives could use to track the elderly person's activity throughout the day. Interviewees were then asked questions about privacy perceptions and opinions. The results suggested that participants were likely to accept potentially invasive technology given an adequate level of trust in the people managing the technology and safety benefits.

According to Spiekerman et al., a fundamental difficulty in probing privacy though scenarios lies in avoiding bias in participants' response [268], particularly for applications that do not yet exist.

3.1.7 Mobile and Location-Enhanced Technologies

We finally explore the problem of understanding user preferences in the domain of mobile and location enhanced applications. In particular, location-enhanced applications have been widely discussed in the media and have been the topic of much research in the fields of security, privacy, systems, and computer networking.

Kindberg et al. conducted evaluations to assess people's perceptions of trust, privacy, and security with respect to electronic payments using wireless point-of-sale terminals in a simulated restaurant setting [174]. Their experiment included demonstrations of different payment methods followed by interviews, sorting exercises, and questionnaires devised to elicit privacy and security perceptions and preferences. Their results show that in the user's view, privacy is mixed with concerns about convenience and social appropriateness [81]. Kindberg et al.'s analysis is interesting because they positioned each participant within a "privacy perception space" defined by the following three dimensions: privacy concerns, desire for convenience, and desire to be socially appropriate.

Location technologies have been a hot topic because of the numerous privacy implications and economic interests involved. In many cases, researchers have employed scenario-based questionnaires or experience sampling to probe location disclosure preferences.

One study, conducted by Lederer et al., found that people were more likely to make a decision about a location disclosure based on *who* was asking rather than *where* the person currently was [194]. Barkhuus and Dey employed a diary to perform an interval-contingent study about the location disclosure preferences in location-based applications [30]. This study was based in part on the Active Campus technology developed at UCSD, which includes a location-aware mobile terminal usable within the university campus. In Barkhuus and Dey's study, participants were asked to fill out, every evening, a diary entry detailing the perceived usefulness and perceived invasiveness of one of two kinds of location-based applications, with reference to the participant's activities during that day. Results showed that an application that tracked the location of the user to send "recommendations" or inform friends was perceived as more invasive than an application that only reacted to the location of the user to set interface operating parameters, such as ringtone volume.

In general, however, users entrust the mobile service provider to provide adequate privacy protection for location information. Kaasinen [170] conducted user focus groups, interviews, and demonstrations of location-based services to probe their usability and privacy concerns. Kaasinen's results show that privacy concerns are often cleared by the trusted relationship between customer and mobile operator, as well as by the oversight of regulatory agencies. These findings suggest that sophisticated technologies devised for protecting location privacy may be unnecessary in the views of most users. It should be noted, though, that Kaasinen's participants were all Finnish, and there may be cultural differences in trying to generalize these findings (for example, to cultures that do not have as much trust in governments and corporations).

Until recently, many researchers had assumed that a fundamental parameter in the disclosure of location information is the degree of precision of the disclosure (i.e., whether the device discloses complete geographical coordinates or only an approximation, such as the city name). Consolvo et al.'s experience sampling study of a location-enhanced person finder found however, that in most cases, participants did not "blur" their location to avoid telling others where they were [59]. Instead, participants would either not respond at all, or provide the other person with the location information that they thought would be most meaningful to the recipient.

The findings of Kaasinen and Consolvo et al. diverge from common wisdom in the privacy community. We believe that these studies are compelling examples of why HCI research is important for furthering understanding of end-user privacy concerns.

3.2 Methodological Issues

In this section, we sketch out some of the methodological issues that arise when studying privacy preferences and concerns.

3.2.1 The Use of Surveys in Privacy Research

Surveys are typically used to probe general opinions about well-known applications (e.g., e-commerce), issues (e.g., identity theft), and concerns (e.g., loss of control). Surveys can be used to efficiently probe the preferences and opinions of large numbers of people, and can provide statistically significant and credible results. However, surveying privacy concerns presents the problem of conveying sufficient and unbiased information to non-expert users so that they can express reasonable and informed preferences. Risk analysis is hard even for experts, let alone individuals unfamiliar with a given domain or application. To address this problem, scenarios have been used to convey contextual information, and can greatly increase the effectiveness and credibility of survey responses, but at the risk of introducing significant bias.

A second limitation of privacy surveys, even those employing scenarios, is that they only collect participants' attitudes, which may be quite different from actual behavior and thus not as useful for furthering understanding and aiding system design. To increase realism, Experience Sampling Method (ESM) studies can be used to probe individuals' feelings, preferences and opinions in a specific setting [307]. Experience Sampling techniques are defined as interval-, signal- and event-contingent, depending on what initiates the self-report procedure (respectively, the elapsing of a predefined time interval, a signal provided by the researchers, or a specific event involving the participant).

Diaries are often used in conjunction with ESM for studying mobile technologies. For example, Barkhuus and Dey employed a diary to perform an interval-contingent study regarding the location disclosure preferences of possible location-based applications [30]. Colbert notes that in diary studies, "the participant is asked a hypothetical question about how they would react were their position information obtained, albeit contextualized in an actual rendezvous" [57]. However, without a working reference technology, recall errors and the hypothetical nature of questions may bias the results. For example, usefulness may be underrated.

Consolvo et al. increased the realism of their ESM study using Palm PDAs that simulated location requests from their friends, family and colleagues at random times [59]. The participants were asked to respond to the request assuming that it had been actually made by the specific individual. However, Consolvo et al. noted that the random simulated requests were often implausible from a social standpoint. To add even more context, Iachello et al. combined event-contingent ESM with experience prototyping [50], calling this technique "paratyping" [154]. A technique similar to paratyping was developed by Roßnagel et al. in the context of IT end-user security evaluation [247].

In related work, Ammenwerth et al. point out that there are inherent tensions in the formative evaluation of IT security mechanisms [18].

When testing IT end-user security, users' reactions and performance must be evaluated on technology that does not exist, and yet the user must be familiar with the technology. Further, tests should include breakdowns that would be unacceptable if they happened in reality. Ammenwerth et al. describe how they used a *simulation study* to conduct this kind of evaluation. In simulation studies, a working prototype is tested by "real users (performing) realistic tasks in a real social context (and subject to) real attacks and breakdowns" [18]. Simulation studies are more complicated and expensive than Iachello's paratypes, because they require careful selection of "expert participants," extensive briefing to familiarize them with the technology, and complex data collection procedures. For this reason, they are best used at later stages of design.

3.2.2 Directly Asking About Privacy vs. Observation

An important issue that needs to be considered in all techniques for understanding and evaluating privacy is that there is often a difference between what people say they want and what they actually do in practice. For example, in the first part of a controlled experiment by Berendt et al. [39], participants indicated their privacy preferences on a questionnaire. Later, the same participants went through a web-based shopping tour and were much more likely to disclose personal information than previously stated. Their explanation is that participants were enticed in disclosing information in view of potential benefits they would receive.

Focus groups can be used to gather privacy preferences [140, 170]. The advantages and drawbacks of focus groups are well known in the HCI and Software Engineering community and are similar in this context [181]. We have found that focus groups on privacy have unique drawbacks, including susceptibility to cross-talk between informants and the fact that conventions of social appropriateness may bias responses to questions that an informant may consider sensitive or inappropriate. For example, when investigating personal privacy issues between different generations of a family, a focus group with both parents and children will provide poor data.

Individual interviews, especially taking appropriate precautions to strengthen informants' trust of the researcher, will result in better information [202]. Still, interviews have other weaknesses. First, the information that can be gained from an interview is limited by people's familiarity with a given system. Second, interviews do not scale well. Third, interviews tend to gather what people say, but not always what they do. Fourth, interviews can be subject to interviewer bias, for example if there is a large difference in age or socio-economic status between interviewee and interviewer.

3.2.3 Controlled Experiments and Case Studies

Controlled experiments can be very useful for understanding privacy behavior and trust determinants. However, it can be difficult to design experiments that are both plausible and elicit realistic responses from credible privacy threats or concerns. One precaution taken by Kindberg et al. was to avoid explicitly mentioning privacy and security to the participants at the outset of the study [174]. The rationale was to avoid leading participants into specific privacy concerns, and rather probe the "natural" concerns of the users. We are not aware of any research proving that participants of studies on privacy should not be explicitly "led into" privacy or security. However, we believe that this is good precautionary practice, and that the topic of privacy can always be brought up after the experiment.

While conducting user studies, it is important to ensure that the tasks used are as realistic as possible, to give greater confidence of the validity of the results. In particular, participants need to be properly motivated to protect their personal information. Participants should also be put in settings that match expected usage. In their evaluation of PGP, Whitten and Tygar asked people to role-play, acting out in a situation that would require secure email [308]. While it is clear that PGP had serious usability defects, it is also possible that participants could have been more motivated if they had a more personal stake in the matter, or could have performed better if they had been placed in an environment with multiple active users of PGP.

As another example, in Egelman *et al.*'s evaluation of Privacy Finder, the authors discovered that individuals were willing to spend a little more money for privacy, by having participants purchase potentially embarrassing items [87, 118]. To make the purchase as realistic as possible, they had participants use their own credit cards (though participants also had the option of shipping the purchased items to the people running the study). This tradeoff in running realistic yet ethical user studies of privacy and security is an ongoing topic of research.

The most realistic observations can be obtained from case studies [101]. Many case studies focus on a specific market or an organization's use or introduction of a specific technology with privacy implications. For example, case studies have been used to discuss widespread privacy policy violations by US airlines [20], the introduction of PKI-based systems in banks [92], and the introduction of electronic patient records in healthcare IT systems [29].

Finally, some researchers have advocated using ethnographic methods, including contextual inquiry [145], to address the weaknesses of interviews. The basic idea is to observe actual users *in situ*, to understand their current practices and to experience their social and organizational context firsthand. Ethnographic methods have been successfully used to study privacy in the context of everyday life [82, 158, 197]. However, committing to this methodological approach requires the researcher to take an exploratory stance which may be incompatible with the tight process requirements of typical IT development. Nevertheless, we believe that this type of exploratory research is important because many privacy issues are still not well understood, and many of our analytical tools still depend on inaccurate and unverified models of individuals' behavior. We return on this point in the conclusion.

3.2.4 Participatory Design and Privacy

Privacy issues can take on a very different meaning within a workplace, where issues of trust, authority, and competition may arise in a way quite different than with family and friends. Participatory design has been used as a way of understanding user needs in such environments, helping to address privacy concerns up front and increasing overall user acceptance of systems.

For example, Muller et al. investigated privacy and interpersonal competition issues in a collaborative project management system using participatory design [211]. They discovered that specific system features could have contradictory effects on privacy. For example, an alert feature could increase the vulnerability of users by letting colleagues set alerts based on one's progress, while simultaneously protecting one from potential embarrassment by letting individuals add alerts based on other people's alerts (e.g., "remind me about this project five days before the earliest alert set on it by anyone else."). This observation is consistent with current sociological thinking, as mentioned earlier in Section 2.3.1 [23, 117].

Participatory design can help uncover and analyze privacy tensions which might go unnoticed at first glance, because representatives of the end-users are involved throughout the design process and can influence technical choices with their values and needs. Clearly, participatory design also carries ethical and political assumptions that may not be appropriate or applicable in all design contexts [269]. Perhaps due to this reason, we did not find many accounts of the use of participatory design for privacy-affecting applications. Consequently, practitioners should evaluate whether this approach can be carried out or not in their specific context.

3.2.5 Ethics and Privacy

Finally, we discuss ethical issues arising during the design and development of IT that may impact the privacy of stakeholders, including research participants and users of future technologies. Specifically, we focus on the problems inherent in the representation of user's opinions, on informed consent of research subjects, and on the issue of deception of subjects.

Many organizations conducting R&D on IT have developed guidelines and procedures to preserve the privacy of research participants and users of prototypes. These guidelines respond to legislation or organizational policy and originate from a long-standing discussion on research ethics. For example, the US Federal Government has issued regulations requiring the protection of research participants' privacy, including the confidentiality of collected data, informed consent procedures, and confidentiality of attribution [76]. These requirements are verified and enforced by so-called "Institutional Review Boards" (IRB), present in most US research organizations.

Mackay discussed the ethical issues related to the use of videotaping techniques for usability studies and prototype evaluation [198]. Drawing on other fields such as medicine and psychology, Mackay suggests specific guidelines for how videos should be captured and used. With respect to research participants' privacy, these guidelines cover issues such as informed consent, purposefulness, confidentiality, further use of the video, misrepresentation, and fairness. Many of MacKay's suggestions overlap with IRB requirements and constitute a commonly-accepted baseline practice for the protection of participants' privacy.

In the past few years, however, researchers have voiced concerns from the application of IRB requirements to social, behavioral, and economic research [56]. In the HCI community, researchers face similar challenges. For example, in a study investigating privacy preferences of a ubicomp application, Iachello et al. encountered problems related to consent requirements set by the IRB. In that case, it was essential that the survey procedure be as minimally invasive as possible. However, the information notice required by the IRB disrupted the experience even further than the disruption caused by filling out the survey [154]. Iachello et al. noted that more concise consent notices would be helpful, though changing standard wording requires extensive collaboration with IRB officials.

Further ethical issues are raised by Hudson et al. [147], who report on a study of privacy in web-based chat rooms. Hudson and Bruckman note that obtaining informed consent from research participants may skew the observations by destroying the very expectations of privacy that are the object of study.

Another ethical issue relates to studies involving participant deception. One remarkable study was conducted by Jagatic et al. at Indiana University to study the behavior of victims of "phishing" schemes. In this IRB-approved study, the researchers harvested freely available data of users of a departmental email system by crawling social network web sites; this allowed the researchers to construct a network of acquaintances for each user. They then sent to these users emails, apparently originating from friends and acquaintances, and asking to input departmental authentication data on a specially set-up web page [160] — a sophisticated phishing scheme. Their results showed remarkable rates of successful deception. Participants were informed of the deception immediately after the study ended and were given the option to withdraw from the study per IRB requirements; a small percentage of participants did withdraw. However, some participants complained vehemently to the researchers because they felt an invasion of privacy and believed that their email accounts had been "hacked."

3.2.6 Conclusions on Methodology

In summary, methodological issues in HCI research relate to privacy in multiple ways. One salient question is whether surveys, focus groups, and interviews should be structured to present both benefits and losses to participants. Clearly, a balanced presentation could elicit very different responses than a partial description. A second ethical question relates to whether uninformed attitudes and preferences should drive design, or whether researchers should only consider actual behavior. These questions are but instances of similar issues identified in user-centered design over the past two decades, but are raised time and again in the context of privacy [70, 267].

Stated preferences vs. actual behavior is another important methodological issue. As Acquisti and Großklags point out, individual decision making is not always rational, full information is seldom available, and the topic is often too complex for the typical user to understand [8]. For these reasons, basing system design on the result of surveys may be potentially misleading. Because of the difficulty of probing behavior, techniques that only probe attitudes toward privacy should be used with great care and the results should be interpreted accordingly.

Third, privacy can be a difficult topic to investigate from a procedural standpoint. Iachello et al.'s and Hudson and Bruckman's experience shows that IRB informed consent requirements may impede achieving the immediacy required for authentic collection of privacy preferences. Second, participant privacy may be violated when following certain protocol designs, even when these protocols are approved by the IRB. We believe that an open discussion on an IRB's role in HCI research on privacy should help evolve current guidelines, often developed for medical-type research, to the dynamic and short-term participant-based research in our field.

3.3 Prototyping, Building, and Deploying Privacy-Sensitive Applications

In this section, we focus on privacy with respect to prototyping, building, and deploying applications. We consider both research on methods (i.e., what processes to use to uncover privacy issues during design) and practical solutions (i.e., what design solutions help protect privacy). Cranor, Hong, and Reiter have sketched out three general approaches to improve user interfaces for usable privacy and security [68]:

- Make it invisible.
- Make it understandable, through better awareness, usability, and metaphors.
- Train users.

These three themes come up repeatedly in the subsections below. It is also worth pointing out user interface advice from Chris Nodder, who was responsible for the user experience for Windows XP Service Pack 2: "Present choices, not dilemmas." User interfaces should help people make good choices rather than making them confused about what their options are and obfuscating what the implications of those decisions are.

Work on privacy-enhancing interaction techniques is quite extensive and we present it here in several subsections. Early Privacy Enhancing Technologies (PETs) were developed with the intent of "empowering users," giving them the ability to determine their own preferences [310]. More recent work has taken a holistic and more nuanced approach encompassing architectural and cognitive constraints as well as the user interface. For example, work on identity management and plausible deniability demands that the whole system architecture and user interface be designed with those end-user concerns in mind [231]. Finally, the reader will note that the literature relating to interaction techniques for privacy is intertwined with that of usable security. This is because security mechanisms are the basic tools of privacy protection. We limit our discussion to interaction techniques specifically targeted at privacy, ignoring other work on topics such as biometrics and authentication if it is not directly connected with privacy.

Finally, we note that there is still a strong need for better tools and techniques for designing, implementing, and deploying privacy-sensitive systems. We discuss these issues as key research challenges in Sections 4.2.2–4.2.5.

3.3.1 Privacy Policies for Products

Publishing a privacy policy is one of the simplest ways of improving the privacy properties of an IT product, such as a web site. Privacy policies provide information to end-users to express informed consent and help products comply with the Openness and Transparency principles of the FIPS.

Privacy policies are very popular on the World Wide Web, both in nations that mandate them whenever personal data is collected (e.g., the EU) and where they are used because of market pressure (e.g., in certain industries in the United States). The specific content and format of privacy policies varies greatly between national contexts, markets, and industries. Under many legal regimes, the content of privacy notices is specified by law, and web site publishers have little leeway in writing them. The objective of these laws is to inform the user of his rights and to provide notices that enable informed consent. In other cases, privacy policies are written with the goal of increasing user trust and have a reassuring, rather than objective, tone. Certification programs such as TRUSTe and BBBOnline also mandate certain minimal requirements for privacy policies. These programs also verify that participating web sites comply with their stated policy, although such verification is “shallow” because the certification programs do not assess the internal processes of the organizations running the web sites.

3.3.1.1 Helping End-Users Understand Privacy Policies

There have been extensive efforts to make policies more understandable by consumers, especially for Business-to-Consumer (B2C) e-commerce web sites. However, the results thus far have not been encouraging. Controlled experiments by Good et al. on End-User Licensing Agreements [124] and by Jensen et al. on web site privacy policies [165] strongly suggest that users tend not to read policies. These studies also indicate that policies are often written in technical and legal language, are tedious to read, and stand in the way of the primary goal of the user (i.e., concluding the transaction).

Evidence external to the HCI field confirms this finding. A 2003 report by the EU Commission showed that eight years after the introduction of the EU data protection directive 95/46, the public is still not knowledgeable of its rights under data protection legislation [58]. This is remarkable, considering that these rights must be repeated to the users in a mandatory privacy policy every time personal information is collected, and that the user must agree with the policy before the collection can take place.

Indeed, the general consensus in the research community is that privacy policies are designed more to shield the operators of IT services from liability than to inform users. Furthermore, Jensen and Potts's evaluation of the readability and usability of privacy policies suggests that current policies are unfit as decision-making tools due to their location, content, language, and complexity [164]. Users instead tend to receive information about privacy-related topics such as identity theft from the media and trusted sources like expert friends.

Multi-level policies have been proposed as one way to increase comprehensibility and the percentage of users reading policies. In 2004, the European Union's committee of data privacy commissioners, also known as the Article 29 Working Party, published a plan calling for EU member states to adopt common rules for privacy policies that are easy for consumers to understand [96]. This plan also called for displaying privacy policies in three layers: short, condensed, and complete. The *short privacy policy*, only a few sentences long, is meant to be printed on a warranty card or sent via a mobile phone message.

It might contain a link to the condensed privacy notice. The *condensed privacy policy* is a half-page summary of the *complete privacy policy.* The condensed privacy policy summarizes the most important points, whereas the complete privacy policy might span multiple pages is comprehensive. Experimental evidence suggests that two-level policies are somewhat more successful at influencing users' behavior [123].[1]

To systematize the wide range of claims contained in privacy policies, Anton and Earp produced a dictionary of privacy claims contained in the privacy policies of 25 major US retailers' web sites [21]. Similar to Dourish et al. [82], Anton and Earp used Grounded Theory and goal mining techniques to extract these claims and produced a list of 124 privacy goals. They categorized claims in privacy policies as "protection goals" (i.e., assertions with the intent of protecting users' data privacy) and "vulnerabilities" (i.e., assertions that describe management practices that may harm user privacy such as sharing of personal information). The privacy goals taxonomy reflects the usual categories of notification, consent, redress, etc., while the vulnerabilities taxonomy includes such issues as data monitoring, aggregation, storage, transfer, collection, personalization, and contact.

The emergent picture is that end-user privacy policies are complex instruments which need careful planning, constant updates, and careful drafting to ensure that users read them, understand them, and use them. Obviously, they must reflect to actual organizational practices, which can be a problem especially in rapidly evolving organizations.

3.3.1.2 Deploying, Managing, and Enforcing Privacy Policies

The mere presence of a privacy policy does not mean that it will be enforced. A full treatment of policy enforcement is outside of the scope of this article, but has wide-reaching implications on information systems design and management. Furthermore, different kinds of enforcement procedures exist depending on the data protection legislation and

[1] Google Desktop's privacy policy brings this structure to the extreme, and prompts the user with the following notice upon installation: "Read This Carefully. It's Not the Usual Yada-Yada."

institutions in place. For example, some companies have a Chief Privacy Officer, whose responsibilities may range from public relations to actual involvement in spelling out and enforcing privacy policies. As another example, in the United States, the Federal Trade Commission has been tasked with enforcing the Children's Online Privacy Protection Act (COPPA), and has actively pursued remedies against businesses that are in violation.

Although the management of personal information has not traditionally been the topic of public research, there have recently been several efforts in this field, specifically in two areas:

- tools for privacy policy creation, enforcement and management, and
- certification of information management practices.

The most significant project in the first area is SPARCLE. The vision of SPARCLE is to provide a bridge between natural language and automatic enforcement systems, such as Tivoli [24]. SPARCLE is currently implemented as a web-based tool for translating privacy policies[2] stated in natural language into machine-readable formats akin P3P [172]. The request for this tool came from professionals of IBM's IT services division, suggesting that even expert consultants may find it difficult to write consistent and complete privacy policies.[3] While the difficulties of professionals drafting privacy policies are not documented in academic literature, our own experience coupled with press coverage suggests that the implementation and enforcement of privacy policies within organizations is a pressing and very challenging issue. See, for example, the recent leaks of personal information at Cardsystems [100] and Choicepoint [149, 298].

SPARCLE has recently undergone tests to evaluate what type of policy statement input modality is most effective, i.e., free-text, where the user types the policy directly in the system, or guided, through menu selections. These tests were aimed at an expert user population

[2] "Privacy policy" here refers to the policy internal to the organization, which describes roles, responsibilities and is used for process definition. This is not the policy written for the data subject and posted on the web site.

[3] J. Karat, personal communication, March 2006.

and measured the time necessary to write a policy and the quality of the resulting statements sets [172].

The second aspect of privacy management relates to the IT and human systems that process and secure personal data within organizations. Unfortunately, public information on this topic is scarce. Furthermore, except for checklists such as the Canadian Privacy Impact Assessment [279], general standards are lacking. For example, Iachello analyzed IS17799, a popular information security best practice standard, *vis-à-vis* data protection legislation. He found that the IS17799 lacks support for several common data protection requirements found in legislation, such as limitation of use or the development of a privacy policy. As a result, Iachello proposed augmenting the standard with additional requirements specifically aimed at privacy [150].

In general, we still see little attention to the problem of managing personal information at the organizational level. Given the attention that the HCI and CSCW communities has devoted to issues such as collaboration and groupware systems, and the progress that has been made in these fields since the 1980's, we believe that HCI research could greatly improve the organizational aspects of personal information management. We believe that the challenge in this field lies in aligning the interests of the research community with the needs of practitioners and corporations. We discuss this point more as an ongoing research challenge in Section 4.4.

3.3.2 Helping End-Users Specify Their Privacy Preferences

Many applications let people specify privacy preferences. For example, most social networking web sites let people specify who can see what information about them. There are three design parameters for such applications, namely when users should specify preferences, what the granularity of control is, and what the defaults should be.

The first question can be reframed by deciding when should pessimistic, optimistic, and interactive style user interfaces be used [132, 236]. The goal of a *pessimistic* style is to prevent security or privacy breakdowns, e.g., denying access to data. For example, some applications ask users to specify privacy preferences immediately after installation. However, defining configurations and policies upfront, before starting to use a product, may be difficult for users because the definition process is taken out of context, when the user does not have sufficient information to take a reasoned decision.

The goal of the *optimistic* style is to help end-users detect misuses and then fix them afterwards. An employee might allow everyone in her work group to see her location, but may add security and privacy rules if she feels a specific individual is abusing such permissions. This kind of interaction style relies on *social translucency* to prevent abuses. For example, Alice is less likely to repeatedly query Bob's location if she knows that Bob can see each of her requests. Section 3.3.8 discusses social translucency in more detail.

The goal of the *interactive* style is to provide enough information for end-users to make better choices, helping them avoid security and privacy violations as well as overly permissive security policies. An example is choosing whether to answer a phone call given the identity of the caller. Here, people would be interrupted for each request and would make an immediate decision. One refinement of this idea is to let end-users defer making privacy choices until they are more familiar with the system, similar to the notion of *safe staging* introduced by Whitten and Tygar [308]. A refinement of this concept are Just-In-Time Click-Through Agreements (JITCTA) adopted by the EU PISA project [230], and later by the EU PRIME "PRivacy and Identity Management for Europe" project [231]. JITCTA are presented to the user at a time when he or she can take an informed decision on her privacy preferences. However, Petterson et al. note that users may be induced to automate their "consent clicks" when presented with multiple instances of click through agreements over time, without really reading their contents [231].

It is likely that all three styles are needed in practice, but the optimal mix that balances control, security and ease of use is currently unclear. Furthermore, some domains may have constraints that favor one style over another.

With respect to the granularity of control, Lederer et al.argue that applications should focus more on providing simple coarse-grained controls rather than fine-grained ones, because coarse-grained controls are simpler to understand and use [192]. For example, providing simple ways of turning a system on and off may be more useful than complex controls that provide flexibility at the expense of usability.

Lau et al. take a different path, distinguishing between *extensive* and *intensional* privacy interfaces [190]. In the context of sharing web browser histories in a collaborative setting, they defined extensive interfaces as those where individual data items (i.e., each URL) are labeled as private or public. In their prototype, this was done by toggling a "traffic light" widget on the browser. In contrast, intensional privacy interfaces allow the user to define an entire set of objects that should be governed by a single privacy policy. In their prototype, this was accomplished with access control rules indicating public or private pages, based on specific keywords or URLs, with optional wildcards.

The third design choice is specifying the default privacy policies. For example, Palen found that 81% of corporate users of a shared calendar kept the default access settings, and that these defaults had a strong influence on the social practices that evolved around the application [226]. Agre and Rotenberg note a similar issue with Caller ID [13]. They note that "if CNID (i.e., Caller ID) is blocked by default then most subscribers may never turn it on, thus lessening the value of CNID capture systems to marketing organizations; if CNID is unblocked by default and the blocking option is inconvenient or little-known, callers' privacy may not be adequately protected." In short, while default settings may seem like a trivial design decision, they can have significant impact in whether people adopt a technology and how they use it.

There is currently no consensus in the research community as to when coarse-grained versus fine-grained controls are more appropriate and for which situations, and what the defaults should be. It is likely that users will need a mixture of controls, ones that provide the right level of flexibility with the right level of simplicity for the application at hand.

3.3.3 Machine-Readable Privacy Preferences and Policies

Given that most users may not be interested in specifying their privacy policy, another line of research has attempted to automate the delivery and verification of policies for web sites. The most prominent work in this area is the Platform for Privacy Preferences Protocol (P3P). P3P lets web sites transmit policy information to web browsers in a machine-readable format. Users can then view policies in a standard format and decide whether to share personal information [66]. Users can also set up their web browser to automate this sharing process.

It is worth noting that the idea of a machine-readable privacy policy has been extended to other domains. For example, both Ackerman and Langheinrich proposed using labeling protocols similar to P3P for data collected in ubiquitous computing environments, to express such things as what data about individuals are available, what kinds of information the infrastructure would record, etc. [2, 187].

Although P3P was developed with feedback from various industrial stakeholders, it has been a hotly contested technology (see Hochheiser for an extensive discussion of the history of P3P [144]). One principled criticism is that automating privacy negotiations may work against users' interests and lead to loss of control. Ackerman notes that "most users do not want complete automaticity of any private data exchange. Users want to okay any transfer of private data" [3].

In practice, P3P has not yet been widely adopted. Egelman et al. indicate that, out of a sample of e-commerce web sites obtained through Google's Froogle web site in 2006 (froogle.google.com), only 21% contained a P3P policy [86]. Reasons may include lack of enforcement [89], lack of motivation to adopt stringent policy automation by commercial players [144], and the lack of appropriate user interfaces for delivering the P3P policy to users and involving them in the decision processes [4].

In our view, there are three main roadblocks to the adoption of P3P. The first issue relates to the ability of users to define and control their preferences intuitively. This difficulty could be addressed through enhancements to the user interface of web browsers. For example, Microsoft Internet Explorer 6.0 only has rudimentary support for P3P privacy preferences, letting end-users simply manage how cookies are sent. Some solutions to this roadblock are discussed in the following section.

The second roadblock is that users may not be sufficiently motivated to use these technologies. Many users do not understand the issues involved in disclosing personal information, and may simply decide to use a service based on factors such as the benefit the service offers, branding, and social navigation. We believe that there are many research opportunities in the area of understanding user motivation with respect to privacy.

The third roadblock is that many web sites owners may not have strong economic, market, and legal incentives for deploying these technologies. For example, they may feel that a standard text-based privacy policy may be sufficient for their needs. Web site owners may also not desire a machine-readable privacy policies, because it eliminates ambiguity and thus potential flexibility in how user data may be used.

3.3.3.1 Privacy Agents

From a data protection viewpoint, a privacy decision is made every time a user or a device under her control discloses personal information. The increasing ubiquity and frequency of information exchanges has made attending to all such decisions unmanageable. User interfaces for privacy were developed in part to cater to the user's inability to handle the complexity and sheer volume of these disclosures.

Early work focused on storing user privacy preferences and automating exchanges of personal data excluding the user from the loop. An example of this is APPEL, a privacy preferences specification language developed by Cranor et al. which can be used to describe and exchange personal privacy preferences [69]. When this model was not widely adopted, researchers started investigating the causes. Ackerman et al. noted that users want to be in control for every data exchange of relevance [3]. The concept of Privacy Critics brings the user back in the loop. Critics are agents that help guide the user in making good choices [4] and were introduced by Fischer et al. in the context of software design [103]. Rather than automating decisions, Privacy Critics warn the user when an exchange of personal data is going to happen. It should be noted that modern web browsers have incorporated the concept of critic for other kinds of data transactions, e.g., displaying non-secure pages and accepting dubious PKI certificates. However, it is also worth pointing out that these types of dialog tend to be ignored by users. This issue is discussed in Section 4.2 as an open challenge for future work.

Following this line of research, Cranor et al. developed an agent called Privacy Bird [65]. Privacy Bird compares a web site's P3P policy with a user's privacy preferences and alerts the user to any mismatches. In designing Privacy Bird, precautions were taken to increase the comprehensibility of the privacy preferences user interface, keeping only the relevant elements of P3P, removing jargon, and grouping items based on end-user categories rather than on P3P structure. Cranor et al. evaluated Privacy Bird according to Bellotti and Sellen's feedback and control criteria [38], and found that users of Internet Explorer with Privacy Bird were more aware about the privacy policies of web sites than those without the Privacy Bird.

In related work, Cranor et al. also developed a search engine that prioritizes search results based on their conformance to the policy defined by the user [51]. An evaluation of this privacy-sensitive search engine showed that when privacy policy information is readily available and can be easily compared, individuals may be willing to spend a little more for increased privacy protection, depending on the nature of the items to be purchased [87, 118].

3.3.4 Identity Management and Anonymization

The concept of "privacy assistants" is also central to work by Rannenberg et al. and Jendricke and Gerd tom Markotten on reachability managers [162, 243]. Jendricke and Gerd tom Markotten claim that PETs can help people negotiate their privacy "boundary" by associating different privacy profiles with several digital "identities."

In this model, users can dynamically define and select privacy profiles, for example, based on the current activity of the user, the web site visited, or the current desktop application used. The interface provides an unobtrusive cue of the current selected identity so that the user can continuously adjust her status. However, it is not clear whether a profile-based approach can simplify privacy preferences. Users may forget to switch profiles, as happens with profiles on cell phones and away messages on IM. Studying user interfaces for managing profiles of ubiquitous computing environments, Lederer et al. found that participants had difficulty predicting what information would actually be disclosed [192]. Furthermore, Cadiz and Gupta, in their analysis of sharing preferences in collaborative settings, discovered that sharing personal information is a nuanced activity [52].

The concept of profiles has been further developed into the more general idea of "identity management." Here, users have several identities, or "personas," which can be used to perform different online transactions. For example, users could have an "anonymous persona" to surf general web sites, a "domestic persona" for accessing retail web sites, and an "office persona" for accessing corporate intranets. Decoupling personas from individuals can reduce the information collected about a single individual. However, identity management technologies are rather complex. So far, allowing easy definition of policies and simple awareness active personas has proven to be a difficult task.

Various designs for identity management have been developed. For example, Boyd's Faceted Id/entity system uses a technique similar to Venn diagrams to explicitly specify different groups and people within those groups [43]. The EU PRIME project has also explored various user interfaces for identity management, including menu-based approaches, textual/graphic interfaces, and more sophisticated animated representations that leverage a town map metaphor [231]. Graphical metaphors are often used with other PETs, e.g., using images of keys, seals, and envelopes for email encryption. However, researchers agree that representing security and privacy concepts often fails due to their abstract nature. For example, Pettersson et al. evaluated alternative user interfaces for identity management, and concluded that it is difficult to develop a uniform and understandable vocabulary and set of icons that support the complex transactions involved in identity management and privacy management.

3.3.4.1 The Challenges of Complex PET UIs

The problem of developing appropriate interfaces for configuration and action is common to other advanced PETs, such as anonymization tools like JAP, ZeroKnowledge, Anonymizer, and Freenet. Freenet, an anonymizing web browsing and publishing network based on a Mix architecture [54], was hampered by the lack of a simple interface. Recently, the developers of Tor, another anonymizing network based on onion routing [122], acknowledged this problem and issued a "grand challenge" to develop a usable interface for the system.[4] Whatever their technical merits, anonymization systems — both free and commercial — have not been widely adopted, meeting commercial failure in the case of ZeroKnowledge [121] and government resistance in other cases (e.g., JAP).

Repeated failures in developing effective user interfaces for advanced PETs may be a sign that these technologies are best embedded in the architecture of the network or product and operated automatically. They should not require installation, maintenance, and configuration. As an example, consider the success of SSL in HTTP protocols versus the failure of email encryption. The underlying technology is quite similar, though email encryption is not automatic and has not seen widespread adoption.

Ubiquitous computing technologies present further challenges for the protection of users' privacy. Location privacy has been a hot topic on the media and the research community following the development of mobile phone networks and the E911 location requirements. There have been several technological solutions for protecting users' privacy in mobile networks. For example, Beresford and Stajano propose the idea of Mix zones, where users are not location tracked with their real identity but with a one-time pseudonym [40]. Gruteser and Grunwald also proposed location-based services that guarantee k-anonymity [133]. Beresford and Stajano claim that using Mix technology for cloaking location information enables interesting applications without disclosing the identity or the movement patterns of the user. Tang et al. suggest that many location-based applications can still work in a system where the identities of the disclosing parties are anonymous — e.g., just to compute how "busy" a place is, such as a part of a highway or a café [276].

[4] R. Dingledine, personal communication 7/8/2005. See also http://tor.eff.org/gui.

Yet, it is not clear whether anonymization technologies will be ever widely adopted. On the one hand, network service providers act as trusted third parties and are bound by contractual and legislative requirements to protect the location information of users, reducing the commercial motivation of strong PETs. In other words, location privacy may already be "good enough." On the other hand, location-based services are not in widespread use, and privacy frictions could arise as more people use these services.

3.3.5 End-User Awareness of Personal Disclosures

Initially focused on network applications (e.g., World Wide Web and instant messaging), work on disclosure awareness has expanded into areas such as identity management systems, privacy agents, and other advanced PETs.

Browser manufacturers have developed artifacts such as the lock icon, specially colored address bars, and security warnings to provide security awareness in browsing sessions. Friedman *et al.* developed user interfaces to show to end-users what cookies are used by different web sites [109].

However, there are few published studies on the effectiveness of these mechanisms. Few notable exceptions include Friedman et al.'s study showing the low recognition rate of secure connections by diverse sets of users [110], and Whalen and Inkpen's experiments on the effectiveness of security cues (the lock icon) in web surfing sessions [306]. Whalen and Inkpen used eye-tracking techniques to follow users' focus of view when interacting with web sites. The results indicate that users do not look at, or interact with, the lock icon to verify certificate information. Furthermore, they showed that even when viewed, certificate information was not helpful to the user in understanding whether the web page is authentic or not.

Recently, interaction techniques for awareness have been developed in the context of ubiquitous computing, because the lack of appropriate feedback is exacerbated by the often-invisible nature of these technologies [300]. Nguyen and Mynatt observed that in the physical world, people can use mirrors to see how others would see them. Drawing on this analogy, they introduced the idea of Privacy Mirrors, artifacts that can help people see what information might be shared with others. According to Nguyen and Mynatt, technology must provide a history of relevant events, feedback about privacy-affecting data exchanges, awareness of ongoing transactions, accountability for the transactions, and the ability to change privacy state and preferences. This framework was used to critique a multi-user web-based application and to develop original design ideas for it [220]. However, the Privacy Mirrors concept itself was not formally evaluated.

An interesting variant of the Privacy Mirror concept is the peripheral privacy notification device developed by Kowitz and Cranor [182]. In this system, a display located in a shared workplace shows words taken from unencrypted chats, web browsing sessions, and emails transiting on the local wireless network. Kowitz and Cranor carefully designed this awareness device so that only generic words are anonymously projected on the display (i.e., no personal names), and words are selected out of context so that the meaning of the phrase is likely not intelligible by others. Kowitz and Cranor assessed the reactions of users through interviews and questionnaires before and after the deployment of the device. The self-reported results indicate that the users of the wireless network became more aware of the unencrypted wireless network, but did not change their usage behavior. Kowitz and Cranor note that the change in perception was likely due to the awareness display since participants already knew that wireless traffic was visible to eavesdroppers. However, awareness was not tied to any actionable items, as the system did not suggest what steps one could take to protect oneself.

A key design issue in awareness user interfaces is how to provide meaningful notifications that are not overwhelming nor annoying. Good et al. showed that end-users typically skip over end-user license agreements [123]. Many users also ignore alert boxes in their web browsers, having become inured to them. Currently, there is no strong consensus in the research community or in industry as to how these kinds of user interfaces for awareness should be built. This issue is discussed as a key challenge for future work in Section 4.1.

For further reading, we suggest Brunk's overview of privacy and security awareness systems [28] and Lederer's examples of feedback systems of privacy events in the context of ubiquitous computing [191].

3.3.6 Interpersonal Awareness

An alternate use of the term "awareness" relates to the sharing of information about individuals in social groups to facilitate communication or collaboration. This type of sharing occurs for example in communication media, including videoconferencing [114, 264], group calendars [34, 282], and synchronous communications [35, 228].

One example of awareness system is RAVE, developed in the late 1980's at EuroPARC [114]. RAVE was an "always on" audio/video teleconferencing and awareness system. Based on the RAVE experience, Bellotti and Sellen wrote an influential paper presenting a framework for personal privacy in audio–video media spaces [38] (see Section 3.5.2). RAVE provided visible signals of the operation of the video camera to the people being observed, to compensate the disembodiment of the observer-observed relationship. Moreover, Bellotti and Sellen also suggested leveraging symmetric communication to overcome privacy concerns. Symmetric communication is defined as the concurrent exchange of the same information in both directions between two individuals (e.g., both are observers and observed).

Providing feedback of information flows and allowing their control is a complex problem. Neustaedter and Greenberg's media space is a showcase of a variety of interaction techniques. To minimize potential privacy risks, they used motion sensors near a doorway to detect other people, weight sensors in chairs to detect the primary user, physical sliders to control volume, and a large physical button to easily turn the system on and off [218].

Hudson and Smith proposed obfuscating media feeds by using filters on the video and audio [148]. These filters include artificial "shadows" in the video image as well as muffled audio. While they did not evaluate these privacy-enhancing techniques, Hudson and Smith posited that privacy and usefulness had to be traded off to achieve an optimal balance. Boyle et al. also proposed video obfuscation to protect privacy for webcams in homes [44, 218]. However, evaluation by Neustaedter et al. showed that obfuscation neither increased users' confidence in the technology nor their comfort level [219]. It is thus not clear whether obfuscation techniques, which are based on an "information-theoretic" view (i.e., disclosing less information increases privacy), actually succeed in assuring users that their privacy is better protected.

The idea of "blurring information" was also proposed in the domain of location information [83, 237]. However, the results of Neustaedter et al. for video are paralleled by results by Consolvo et al. in location systems [59]. Consolvo et al. discovered that users disclosing location seldom make use of "blurring" (i.e., disclosing an imprecise location, such as the city instead of a street address), in part for lack of need and because of the increased burden on usability.

Tang et al. suggest using "Hitchhiking" as an alternative approach: rather than modulating the precision of location disclosures, the identity of the disclosing party along with any sensed data is anonymized [276]. This approach can still support a useful class of location-based applications, ones that focus on places rather than on individuals. For example, a count of the number of wireless devices in a space could indicate how busy a coffee shop is.

More recent work has investigated how a caller can assess the receiving party's availability to communicate, by providing information about the context of the called party. See, for example, Schmandt et al.'s Garblephone [254], Nagel's Family Intercom [215], Avrahami et al.'s context cell phone protocol [26]. Milewski and Smith included availability information in shared address books [206]. Schilit provides a survey of these kinds of context-aware communication, observing that increased awareness can be useful, though at the cost of privacy [253]. In fact, these systems have contradictory effects on privacy perceptions (Section 2.3.1). On the one hand, they can increase environmental privacy because the caller can choose not to disturb the recipient if she is busy. On the other hand, these awareness systems cause information about individuals to be communicated automatically and reduce plausible deniability.

More recently, Davis and Gutwin surveyed disclosure preferences of awareness information. They asked individuals what types of awareness information they would disclose to seven different relationship types and found that most individuals would allow decreasing amounts of information to weaker relationships [75]. Yet, Nagel observed, based on extensive user studies, that individuals may not want to share availability information due to a perceived lack of usefulness of such information [213]. Nagel's results suggest that the utility and drawbacks of these systems are yet unclear.

3.3.7 Shared Displays: Incidental Information and Blinding

A common problem encountered when several individuals are viewing the same computer screen is that potentially private information, such as bookmarks or financial information, may be accidentally disclosed. This issue may arise due to multiple people using the same computer, when projecting a laptop onto a larger screen, or "shoulder surfing," in which a bystander happens to see someone else's screen. Some on-the-road professionals apply a physical filter on their laptop screens. Similarly, blinders are GUI artifacts that hide parts of the user interface to block view of sensitive information. Tarasewich and Campbell proposed using automatic blinders to protect personal data in web browsers [277]. Sensitive information is first identified using pattern recognition. This information can be redacted with black rectangular blocks or encoded using a set of secret colors. Experimental results suggest that these techniques are surprisingly usable in everyday tasks.

Similarly, Miller and Stasko used coded displays for sensitive information shown in semi-public peripheral displays [270]. In their Infocanvas system, sensitive information such as stock quotes is depicted in a graphical, artful way (e.g., by a cloud hovering over a landscape), using a secret code. While not "strong" from a security standpoint, this technique may be acceptable for many deployment settings.

Schoemaker and Inkpen developed an alternative approach for displaying private information on shared displays using blinding goggles typically used for achieving stereoscopic 3D vision on traditional computer screens [259]. The display shows public data to all viewers and private data only to the users whose goggles are currently transparent. Ideally, a system would be able to quickly multiplex all these views on the same display. Schoemaker and Inkpen evaluated the system using a collaborative game and found it to be usable by the participants. They also claim that mixed shared/public displays could provide opportunities for enhanced collaboration, supporting both shared data and individual exploration and elaboration of the data.

The proliferation of personal, semi-public and public displays suggests that blinding and coding may become common techniques in the HCI privacy landscape.

3.3.8 Plausible Deniability, Ambiguity, and Social Translucency

Past work by Hindus et al. in the home [143] and by Hong for location-based services [146] suggested a social need to avoid potentially embarrassing situations, undesired intrusions, and unwanted social obligations. Plausible deniability has been recognized as a way of achieving a desired level of environmental and personal privacy in a socially acceptable way [293].

This ambiguity is the basis for plausible deniability in many communication systems. For example, Nardi et al. observed that people could ignore incoming instant messages without offending the sender, because the sender does not know for certain whether the intended recipient is there or not [216]. Consequently, failing to respond is not interpreted as rude or unresponsive. Traditionally, ambiguity has been considered a negative side-effect of the interaction between humans and computers. Recently, however, researchers have recognized that ambiguity can be a resource for design instead of a roadblock. Gaver et al. claim that ambiguity not only provides a concrete framework for achieving plausible deniability, but can enrich interpersonal communications and even games [113].

Several accounts of ambiguity in voice-based communication systems have been documented [22]. For example, the affordances of cell phones enable a social protocol that allows individuals sufficient leeway to claim not having heard the phone ringing. Successful communication tools often incorporate features that support plausible deniability practices [136].

Researchers have attempted to build on the privacy features of traditional Instant Messaging by adding explicit controls on the availability status of the user, though with varying success. For example, Fogarty et al. [105] examined the use of contextual information, such as sound and location information, to provide availability cues in MyVine, a client that integrates phone, instant messaging, and email. Fogarty et al. discovered that users sent IM to their communication partners even if they were sensed as "busy" by the system. Fogarty attributes this behavior to a lack of accountability, in that telling senders that they should not have sent the message may be considered more impolite than the interruption itself.

When plausible deniability mechanisms become explicit, they can lose much of their value. For example, the Lilsys system by Begole et al. uses a traffic sign metaphor to warn others of one's unavailability for communication [35]. Begole et al. report that the traffic signs metaphor was not well liked by participants in a user study. More importantly, users "expressed discomfort at being portrayed as unavailable." Begole et al. believe this discomfort was due to a social desire to appear approachable. Overall, this result suggests that people prefer the flexibility of ambiguity over a clear message that offers no such latitude.

It is also worth noting that plausible deniability is at odds with a traditional view of security, defined as "confidentiality, integrity, and availability" [94]. Integrity and availability contrast with the idea that individuals should be granted a certain amount of unaccountability within information systems. Social science suggests, however, that plausible deniability is a fundamental element of social relations. Thus, plausible deniability should be viewed as a possible requirement for information technology, especially for artifacts meant to support communication between individuals and organizations.

A related issue is that plausible deniability may inhibit *social translucency*, which has been touted as one of the characteristics that makes computer mediated communications effective and efficient. Erickson and Kellogg define *socially translucent systems* as IT that supports “coherent behavior by making participants and their activities visible to one another” [90]. Plausible deniability may make it hard to hold other people accountable for their actions in such systems. A similar tension is explicitly acknowledged in the context of CSCW research by Kling [176] and was debated as early as 1992 at the CSCW conference [15]. It is currently not clear what the best way of balancing these two design features is. Social translucency is also discussed with respect to evaluation in Section 3.3.3.

Finally, one must take into consideration the fact that users of computer-mediated communications systems often perceive to be more protected than what the technology really affords. For example, Hudson and Bruckman show that people have a far greater expectation of privacy in Internet Relay Chat than can be realistically provided given the design and implementation of IRC [147]. Thus, in addition to balancing plausible deniability with social translucency, designers must also consider *users' expectations* of those properties. We concur with Hudson and Bruckman that more research is necessary in this field. This point is raised again in the final part of this article.

3.3.9 Fostering Trust in Deployed Systems

The issue of trust in IT is a complex and vast topic, involving credibility, acceptance, and adoption patterns. Clearly, respecting the privacy of the user can increase trust in the system. The relationship also works in the opposite direction: if an application or web site is trusted by the user (e.g., due a reputable brand), privacy concerns may be assuaged. In this section, we provide a brief overview of HCI research on technology and trust with respect to information privacy, both as a social construct and as a technical feature.

Trust is a fundamental component of any privacy-affecting technology. Many PETs have been developed with the assumption that once adopted, users would then use IT services with increased trust [234]. One particularly interesting concept is that of trust distribution, where information processing is split up among independent, non-colluding parties [54]. Trust distribution can also be adapted to human systems, e.g., assigning two keys to a safe to two different managers.

Social context is another factor impacting trust and privacy. Shneiderman discusses the generation of trust in CSCW systems [258], claiming that just like a handshake is a trust-building protocol in the real world, it is necessary to create "new traditions" and methods for computer-mediated communication. Management science has also explored the differences of meetings that are face-to-face versus using some form of telepresence, such as a phone or videoconference [36, 292]. These studies have generally concluded that for initial or intensive exchanges, in-person meetings are more effective at generating trust.

An interesting example of how social context affects the operation of IT can be seen with an experimental "office memory" project at an Electricité de France research lab [185]. The employees developed and used an audio–video recording system that continuously archived everything that was said and done in the lab. Access to the recordings was unrestricted to all researchers of the lab. The application was used sparingly and generally perceived as useful. An interesting privacy control was that every access to the recordings would be tracked, similar to the optimistic security protocol [236], and that each individual would be informed of the identity of the person looking up the recordings of her workstation. This feature reduced misuse by leveraging existing privacy practices.

Leveraging the *social context* of the office memory application was essential for its acceptance. Acceptance would likely have been very different if the technology had been introduced from the outside or to people who did not trust its management and operation. In fact, Want et al. reported resistance in the deployment of the Active Badge system roughly 15 years earlier at Olivetti Research Labs [294].

It is also worth noting that many criticisms of the original work on ubiquitous computing at PARC came from researchers in a different lab than the one actually developing the systems [137]. Two explanations are possible. First, in some regards, the lab developing the ubiquitous computing systems was engaging in a form of participatory design with their own lab members, increasing adoption and overall acceptance. Second, some members of the other lab felt that the system was being imposed on them.

Persuasiveness is an important factor influencing user perceptions about a technology's trustworthiness [106]. Given the power of perceptions in influencing decisions on privacy preferences, it should not be surprising that relatively weak items, such as the mere presence of a privacy policy or having a well-designed web site, can increase the confidence of users with respect to privacy. Privacy certification programs can increase user trust. There are various types of certification programs for privacy, targeting organizations as well as products (e.g., TRUSTe and BBBOnline). A good summary of these programs is provided by Anton and Earp [21].

Rannenberg proposed more stringent certification [242].[5] The idea behind these efforts is that IT systems could be evaluated by independent underwriters and granted a "certificate," which would promote the products in the marketplace and increase user confidence. This certification focuses on IT *products*. However, the *management* of IT is much more to blame for privacy infringements rather than the actual technical properties of the technology [150]. Iachello claims that sound personal information management practices should be included in security management standards such as IS17799 [157].

In summary, a variety of factors influence end-user's trust in a system. In our opinion, however, strong brands and a positive direct experience remain the most effective ways of assuring users that sound organizational information privacy practices are being followed.

3.3.10 Personalization and Adaptation

Personalization and adaptation technologies can have strong effects on privacy. The tension here is between improving the user experience (e.g., recommendations) and collecting large amounts of data about the user behavior (e.g., online navigation patterns). For example, Kobsa points out that personalization technologies "may be in conflict with privacy concerns of computer users, and with privacy laws that are in effect in many countries" [179].[6] Furthermore, Kobsa and Shreck note

[5] See also the Privacy Enhancing Technology Testing & Evaluation Project. http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15495 (Last visited 7/4/2006).

[6] For an overview of work in this area, we refer [49].

that users with strong privacy concerns often take actions that can undermine personalization, such as providing false registration information on web sites [180]. Trewin even claims that control of privacy should take precedence over the use of personal information for personalization purposes, but acknowledges that such control may increase the complexity of the user interface [281].

Several solutions have been developed to protect users while offering personalized services. For example, Kobsa and Shreck's anonymous personalization services use cryptographic techniques [180]. However, Cranor points out that these strong anonymization techniques may be too complex for commercial adoption [63]. Cranor also observes that privacy risks can be reduced by employing pseudonyms (i.e., associating the interaction to a persona that is indirectly bound to a real identity), client-side data stores (i.e., leveraging user increased control on local data), and task-based personalization (i.e., personalization for one single session or work task).

Notwithstanding Kobsa and Schreck's and Cranor's work, real-world experience tells us that many users are willing to give up privacy for the benefits of personalization. One need only look at the success of Amazon.com's recommender system as an example. Awad and Krishnan provide another perspective on this argument. Their survey probed users' views on the benefits of personalization and their preferences in data transparency (i.e., providing to users access to the data that organizations store about them and to how it is processed) [27]. Awad and Krishnan concluded that those users with the highest privacy concerns ("fundamentalists"), would be unwilling to use personalization functions even with increased data transparency. They suggested focusing instead on providing personalization benefits to those users who are unconcerned or pragmatists and to ignore concerned individuals. Awad and Krishnan's article also includes a brief overview of privacy literature in the MIS community.

Trevor et al. discuss the issue of personalization in ubicomp environments [280]. They note that in these environments, an increasing number of devices are shared between multiple users and this can cause incidental privacy issues. In their evaluation, Trevor et al. probed the personalization preferences of users of a ubiquitous document sharing system in an office setting. They discovered that privacy preferences depend not only on whether the personalized interface runs on a fixed terminal or a portable device, but also on its location and on its purpose of use.

In summary, research in this area suggests that the issue of personalization and privacy is highly contextual and depend heavily on trust, interpersonal relations, and organizational setting. The evidence also suggests that users and marketers alike appreciate customized services. Finally, it is also not clear if sophisticated PETs are commercially viable. Consequently, a normative approach to preventing misuse of personal information might be better advised.

3.4 Evaluation

In this section, we outline significant work either evaluating PETs or specifically probing the privacy characteristics of general applications.[7] Most PETs require advanced knowledge to use, are complex to configure and operate correctly, and ultimately fail to meet end-user needs. However, it is worth pointing out that there are also many examples of IT applications which successfully integrate privacy-enhancing functions, for example instant messaging clients and mobile person finders.

While some researchers had pointed out the importance of user-centered design in security technology [315], only recently has the security and privacy communities started moving down this path. Unfortunately, since many security applications are developed commercially, the results of in-house usability tests, interviews, and heuristic evaluations are not available. User testing of the privacy-related aspects of applications is difficult due to various reasons, including their non-functional nature and their prolonged appropriation curves. As a result, there are not many reports available describing summative evaluation work on PETs and privacy-sensitive technologies.

[7] We are aware that the distinction between design and evaluation is, to a certain degree, artificial in an iterative development model. However, we feel that the techniques that are discussed here specifically apply to already-developed products, i.e., are more appropriate for summative evaluation.

3.4.1 Evaluation of User Interfaces

One of the earliest and most renowned papers discussing HCI issues and PETs was Whitten and Tygar's "Why Johnny Can't Encrypt" [308]. Whitten and Tygar reported on the usability of Pretty Good Privacy (PGP), a popular email encryption application [313]. They conducted a cognitive walkthrough and a lab-based usability test on PGP. In the usability test, experienced email users were asked to perform basic tasks, for example, generating keys and encrypting and decrypting emails. Results showed that a majority of users did not form a correct mental model of the public-key encryption process. Some users also made significant mistakes such as sending unencrypted email, while others did not manage to send mail at all within the time limit.[8]

Friedman et al. have studied the user interfaces for web browsers' cookie handling in depth. Millett, Friedman, and Felten, for example, studied how the notification interfaces for cookies changed between 1995 and 2000, both in Netscape's and Microsoft's web browsers [207]. Expert analysis of UI metrics, including depth of menu items for configuration and richness of configuration options, showed that significant changes ensued over this five-year period. Configuration options were expanded, which Millett et al. consider a positive development. Further enhancements include better wording for configuration options and more refined cookie management (e.g., allowing users to delete individual cookies). Providing users more choice and better tools to express informed consent clearly comports with Value Sensitive Design [109].

[8] While low usability certainly contributed to PGP's lackluster adoption, it is also likely that a reverse network effect, where few people could decrypt email, coupled with a perceived lack of need may also be responsible. For example, it is worth noting that the competing S/MIME standard, already integrated in popular email applications like Outlook and Thunderbird, has also not yet been widely adopted, notwithstanding the fact that it is arguably simpler to use (although not necessarily to configure).

Generally speaking, email encryption systems have been most successful when a service organization was present to configure and set up the clients. However, Gaw et al. found that even in organizations where email encryption technology is used, decisions about encrypting emails were driven not just by technical merit, but also by social factors [115]. They found that "users saw universal, routine use of encryption as paranoid. Encryption flagged a message not only as confidential but also as urgent, so users found the encryption of mundane messages annoying." Interestingly, this result is paralleled by research by Weirich and Sasse on compliance with security rules — users who follow them are viewed as paranoid and exceedingly strict [299].

However, the evaluation of PGP, discussed above, suggests that UI complexity is a fundamental drawback of these technologies and that PETs might be more effective with fewer, rather than more, choices. As noted in Section 3.2, systems should present meaningful choices rather than dilemmas.

In related research, Whalen and Inkpen analyzed the usage of security user interfaces in web browsers, including the padlock icon that signals a HTTPS connection with a valid certificate [306]. Using eyetracker data, they found that while the lock icon was viewed by participants, the corresponding certificate data was not. In fact, participants rarely pulled up certificate information and stopped looking for security cues after they have signed into a site. Complexity may be again a culprit here, considering that web browser certificate information dialogs are typically difficult to interpret for all but the most security savvy users.

The same theme of configuration complexity emerges from Good et al.'s work on the privacy implications of KaZaA, a popular file-sharing network [124]. Good et al. performed a cognitive walkthrough of the KaZaA client as well as a laboratory user study of its user interface. Results showed that a majority of participants were unable to tell what files they were sharing, and some even thought that they were not sharing any files while in fact all files on their hard drive were shared. Good et al. also probed the KaZaA network, finding that in fact a large number of users "appeared to be unwittingly sharing personal and private files, and that some users were [...] downloading files containing ostensibly private information." In summary, Whitten and Tygar's, Whalen et al.'s, and Good et al.'s findings all indicate that privacy-affecting technologies are easily misunderstood and that their safe use is not obvious.

Difficulties in comprehension affect not only PETs but also privacy policies. Jensen and Potts analyzed 64 privacy policies of both high-traffic web sites and web sites of American health-related organizations (thus subject to HIPAA) [164]. They analyzed policy features including accessibility, writing, content, and evolution over time. The results portray a rather dismal situation. While policies are generally easy to find, they are difficult to understand. The surveyed policies were in general too complex from a readability standpoint to be usable by a large part of the population, which Jensen and Potts note also questions their legal validity. Furthermore, the user herself is typically responsible for tracking any changes to policies, thus curtailing effective notification. The policies of some web sites were very old, exposing both users and site operators to potential risks (respectively, unauthorized uses of personal information and legal liability). Finally, Jensen and Potts note that users typically do not have the choice to decline terms of the policy if they want to use the service. In short, the resulting picture is not encouraging. Users may well be responsible for not reading privacy policies [123], but even if they did, they would find it difficult to understand them, track them over time, and resist accepting them.

Evaluation of privacy-sensitive IT applications has also extended to off-the-desktop interaction. For example, Beckwith discusses the challenges of evaluating ubiquitous sensing technologies in assisted living facilities [33]. Beckwith deployed an activity sensing and location tracking system in a facility for elderly care, and evaluated it using semiformal observation and unstructured interviews with caregivers, patients, and their relatives. One question that arose was how users can express informed consent when they do not understand the operation of the technology or are not aware of it. Their observations highlight the users' lack of understanding with respect to the recipient of the data and its purpose of use. Beckwith proposed renewing informed consent on a regular basis, through "jack-in-the-box" procedures — an approach that resembles the Just-In-Time Click-Through Agreements of Patrick and Kenney [230].

In conclusion, existing work evaluating privacy-affecting technologies shows that these technologies are too demanding on users [91]. Besides establishing common practices and safe defaults, we need to define appropriate metrics on user understanding and ability to express consent, and consistently try to improve them over time.

3.4.2 Holistic Evaluation

In addition to basic usability, applications must also be evaluated in their overall context of use. One key aspect of holistic evaluation is understanding the social and organizational context in which an application is deployed, because it can affect acceptance and skew the results of an evaluation (e.g., Keller's analysis of privacy issues of electronic voting machines [173]). This kind of analysis is often done with retrospective case studies and controlled deployments of prototypes [48], and is challenging due to the temporal timeframe of the evaluation and complex data collection methods.

One interesting example of how social context affects the acceptance of privacy-sensitive IT is provided by the "office memory" project developed at the Laboratory of Design for Cognition at Electricité de France [185] discussed in Section 3.2.9. Here, the *social context* was essential for acceptance: the users were by and large the builders of the application. It is likely that acceptance would have been much lower in another setting. For example, as noted in Section 3.3.9, there was much resistance to the deployment of the Active Badge system [294] outside of the group that developed it [137]. Perception of individual autonomy, political structures, and group tensions all contributed to the rejection of a technology that was perceived as invasive.

Similarly, in hospitals, locator badges are used to facilitate coordination and protect nurses from spurious patient claims. However, in many cases, these locator badges have led to increased friction between workers and employers, as they were perceived by nurses as a surreptitious surveillance system [16]. In at least two separate cases, nurses outright refused to wear the locator badges [16, 53]. In cases where the value proposition was clear to the nurses using it, and where management respected the nurses, the system was accepted. In cases where the value proposition was not clear or was seen as not directly helping the nurses, the system tended to exacerbate existing tensions between the staff and management.

A second contentious social issue with respect to privacy-invasive systems is adjudication, that is, whose preferences should prevail in situations where part of the user base favors a technology and part opposes it. Although a general discussion is beyond the scope of this paper, one interesting comment is made by Jancke et al. in the context of a video awareness systems [161]. Jancke et al. note that what is commonly considered a public space is not one-dimensionally so. A vocal minority of their users were unsettled by an always-on system linking two public spaces. These users felt that there were many private activities that took place in that "public space" such as personal phone calls, eating lunch, and occasional meetings, and that the private nature of this "public space" was being subverted. Before the video awareness system was deployed, there was a degree of privacy based on the proxemics of the space. However, when computer-mediated communication technologies are introduced, such privacy was destroyed because individuals could not easily see who was present at the other end of the system. This shows that a legal or technical definition of public space often does not align with people's expectations.

A third key aspect of holistic evaluation stems from the observation that privacy and security features are often appropriated late in the learning curve of an application [153], often after some unexpected security or privacy "incident." Forcing participants to use privacy-related features can speed up the evaluation, but may be detrimental because the participants' attention is focused on a specific feature instead of the whole application. Thus, the evaluation of privacy and security through test deployments requires researchers to engage in the observation of prolonged and continued use.

For example, Ackerman et al. performed a field study of an "audio media space" over the course of two months [6]. Their system provided an always-on audio communication link between remote co-workers. Users' experiences were studied through interviews, transcripts of communications, usage logs, and direct observation [142]. Ackerman et al. report the gradual emergence of social norms regulating the use of the space by group members. Users started ignoring disclosures by other users that were clearly personal in nature and had been transmitted through the system by mistake, perhaps because one party had forgotten to turn off the media space before a sensitive conversation.

Cool et al. also discuss the long-term evaluation of a videoconferencing system developed at Bellcore during the 1990's [60]. The system started out as an always-on link between public spaces and evolved into a personal videoconferencing system on personal workstations. Cool et al. observed four issues with their videoconferencing systems: system drift (system use and norms evolve over time), conflicting social goals of one user within the social system, concerns of social appropriateness and evaluation, and reaching a critical mass of users. Cool et al. point out that test implementations should be as complete and robust as possible, i.e., real products, if credible observations of social behavior are sought. Studies should also extend over a long timeframe to subatantiate conclusions about the system's acceptance. Finally, technology must be evaluated in the context of planned use rather than in a laboratory.

Cool et al.'s work leads to a final aspect of holistic evaluation, namely that it can be difficult to gather data on the privacy-sensitive aspects of IT applications. First, privacy and security are non-functional properties which may not be obvious to the user and might not be obvious in the UI. Second, case studies on privacy and security are often hampered by the lack of public knowledge on failures or successes. Third, concerns of social appropriateness can affect perceptions as well as cause tensions in collaborative environments, all of which can affect observations. These factors suggest that, to interpret observations correctly, researchers must take a broad view of the application and its perceived properties. Only through careful observations will user privacy concerns and perceptions emerge from product evaluations.

3.4.3 The Tension between Transparency and Privacy

In Section 3.2.8, we briefly touched on the tension between privacy and social transparency. One of the goals of CSCW research is to increase communication opportunities through technology. However, increased transparency, e.g., in the form of awareness of others' activities, can conflict with an individual's need for autonomy and solitude, with detrimental effects on organizational effectiveness. To a degree, these tensions have always existed, but Grudin points out that electronically collecting and distributing data about individuals significantly increases the risk of undesired uses [130]. The point of this section is to show that the tension between transparency and privacy is subtle and that simple design features can often make the difference between accepting and rejecting a system.

Groupware calendars provide a prime example of this tension. Two obvious advantages of group calendars are more effective planning and better access to colleagues. However, these advantages also impact users' personal space and work time. Palen describes the prolonged use of a groupware calendar system within a large organization, based on observations and expert analysis [226]. She points out that technological infrastructure can curb risks by making misuse too expensive in the face of the potential gains. She identifies three techniques to achieve this goal. First, Palen proposes limiting calendar "surfing," that is, accessing others' calendar information without a specific need and knowledge of that person. Second, privacy controls should be reciprocal, meaning that social subgroups share the same type of information in a symmetric way. Finally, social anonymity helps prevent systematic misuse. Palen notes that calendars were retrieved based on a specific employee name. Consequently, while any employee could in theory access any other employee's calendar, this rarely happened since he would only know the names of a limited number of people in the company.

Tullio discusses a groupware calendar used to predict other users' availability, for purposes of initiating in-person or mediated communication [282]. In addition to a qualitative analysis, Tullio performed an expert analysis of his groupware calendaring application using Jensen's STRAP method and identified several potential privacy vulnerabilities, including prediction accuracy, consent, and notification. Tullio also notes that in these kinds of systems, concerns arise for "both [. . .] controlling access as well as presenting a desired impression to others." These dynamics are related to Goffman's work on presentation of self and to the concept of personal privacy we outlined in Section 2.2.2.

An explicit analysis of varying degrees of social transparency is encompassed in Erickson et al.'s work on socially translucent systems [90]. In socially translucent systems, the overall goal is to increase awareness and communication opportunities by presenting information about others' activities. These systems are translucent[9] since they only present select aspects of activity, as opposed to being "transparent" and presenting all aspects [46]. Erickson et al. developed Babble, a chat system that allows one-to-one and group communication. Babble stores a

[9] The concept of translucency has also been used in other HCI domains with different meanings, for example in the design of user interfaces for mobile systems [85].

persistent, topic-threaded copy of the chats, and offers a graphical representation of users that provides awareness of their activity within the chat system. The system was used for over two years within the research organization of the authors. Thus, observations of Babble's use were grounded in an extensive deployment that saw both adoption successes in some groups and failures in other groups. The authors report that the system was often used to initiate opportunistic interactions, and contributed to increasing group awareness while preserving a sufficient degree of privacy for the involved parties.

One interesting aspect of Erickson et al.'s work is that they claim to have willfully refrained from building norms and social conventions in the UI and system architecture. For example, Babble did not provide specific tools for protecting privacy, expecting instead that users would develop their own acceptable behaviors and norms around the system. They argue that this did indeed happen. In fact, Erickson et al. go as far as stating that building such privacy-protecting mechanisms would have prevented users from showing one another that they could be trusted in their use of the system, a process that strengthened rather than weakened the social bonds within the organization [90]. Clearly, such an approach is possible only in specific contexts which should be carefully evaluated by the designer.

In many cases, though, privacy-enhancing features cannot be avoided. However, simple privacy precautions are often sufficient. An example is provided by Grasso and Meunier's evaluation of a "smart" printing system deployed at Xerox R&D France [125]. Their printing system has two main functions: it stores printed jobs on the print server for future access, and has an affinity function that shows, on the header page of each print job, information about similar print jobs submitted by other users. The objective of the latter function is to enable social networking between people interested in the same type of information. Grasso and Meunier claim that the simple privacy-enhancing features built in the system are sufficient for preventing abuse. First, users must intentionally use the "smart printer." Regular printers are still available. Second, a "forget" function is available that removes any trace of the print history of a specific user.

In conclusion, the examples above show that the interaction between social norms and technology is often subtle. Privacy by obscurity, such as in Palen's case study, can effectively curtail privacy violations, even if it is not a "strong" mechanism. Erickson et al.'s work suggests that technology should leverage, rather than mechanically reproduce, social norms. Finally, designers should remember that often simple UI features are sufficient to curtail misuse, as Grasso and Meunier's experience shows.

3.5 Privacy Frameworks

Unlike other areas of HCI, there are few widely accepted frameworks for privacy, due to the elusiveness of privacy preferences and the technical hurdles of applying guidelines to specific cases. In this section, we discuss some of the frameworks that have been proposed to analyze and organize privacy requirements, and note the benefits and drawbacks of each (see Table 3.2).

Privacy frameworks relevant to HCI researchers and practitioners can be roughly grouped into three categories. These include *guidelines*, such as the aforementioned Fair Information Practices [225]; *process frameworks*, such as Jensen's STRAP [166] or Bellotti and Sellen's Questions Options Criteria (QOC) process [38]; and *modeling frameworks*, such as Jiang et al.'s Approximate Information Flows [168].

These frameworks are meant to provide guidance for analysis and design. However, it should be noted that few of these frameworks have been validated. By validation, we mean a process that provides evidence of the framework's effectiveness by some metric, for example design time, quality of the overall design, or comprehensiveness of requirements analysis. In most cases, these frameworks were derived based on application practice in related fields or from the authors' experiences.

This lack of validation partially explains why many frameworks have not been widely adopted. Indeed, case studies have been better received. Nevertheless, the issue of knowledge reuse in HCI is pressing [273] and accounts of single applications are not an efficient way of communicating knowledge. We believe that research on privacy can greatly benefit from general guidelines and methods, if they are thor-

Table 3.2 Overview of HCI privacy frameworks.

Framework name	Scope	Data protection/ personal privacy	Principled/ communitarian	Advantages	Disadvantages
Guidelines					
FIPS	Basic personal data management principles	Data protection	Principled	Simple popular	System-centered Do not consider value proposition
Design patterns (Chung)	Ubiquitous computing	Personal	Principled	Easy to learn	Mismatch with design
Process frameworks					
QOC (Bellotti)	Questions and criteria for evaluating designs	Personal	Principled	Simple	Limited to VMS systems
Risk analysis (Hong)	Ubiquitous computing	Neutral	Communitarian	Clear checklists	Difficult to valuate risk
Privacy Interface Analysis	Web applications	Data protection	Principled	Good rationale	Complex to apply
Proportionality	Value proposition balanced with privacy risk	Neutral	Communitarian	Lightweight. Used in related communities. Explicit balance	Demands in-depth analysis
STRAP	Privacy analysis based on goal analysis	Neutral	Neutral	Lightweight	Goal-driven May ignore non-functional issues

Table 3.2 (*Continued*).

Framework name	**Scope**	**Data protection/ personal privacy**	**Principled/ communitarian**	**Advantages**	**Disadvantages**
Modeling frameworks					
Economic frameworks	Models of disclosure behaviors	Data Protection	Communitarian	Simple economic justification Compatibility with risk reduction cost metrics	Frail assumptions of user behavior
Approximate Information Flows	Model of information flows	Data Protection	Principled	Comprehensive framework	Frail assumptions Incompatible with data protection law
Multilateral security	General model	Neutral	Communitarian	Explicit balance	Lack of process model

oughly tested and validated, and if practitioners and researchers use them with an understanding of their performance and limitations. In fact, we suggest in the conclusion that the development of a *privacy toolbox* composed of several complementary techniques is one of the main research challenges of the field.

3.5.1 Privacy Guidelines

Privacy guidelines are general principles or assertions that can be used as shortcut design tools to

- — identify general application requirements prior to domain analysis;
- — evaluate alternative design options;
- — suggest prepackaged solutions to recurrent problems.

We discuss below the FIPS, design patterns and two sets of specific guidelines for ubiquitous and location-based applications.

3.5.1.1 Fair Information Practices

The Fair Information Practices (FIPS) are among the earliest guidelines and were influential on almost all data protection legislation. The FIPS were developed specifically to help design large databanks of personal information, such as health records, financial databases, and government records (Table 3.3).

The FIPS are the only framework that has been used extensively in industry and by regulatory entities. Data Protection Authorities (DPA) use these guidelines to analyze specific technologies [95, 97]. The EU Art. 29 Working Party bases its analyses on a case-by-case application of the FIPS, along with other principles such as legitimacy and proportionality. The FIPS have also been adapted over time to novel technologies [112, 186] and processes (e.g., Privacy Incorporated Software Agents) [230].

However, given their orginal purpose, the FIPS adopt a data protection and systems-centered viewpoint that may not be appropriate for other applications. The FIPS only suggest evaluating if data collection

Table 3.3 The fair information practices (FIPS), OECD [225] version.

Principle	**Description**
Collection limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use limitation	Personal data should not be disclosed, made available or otherwise used [...] except (a) with the consent of the data subject; or (b) by the authority of law.
Security safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual participation	An individual should have the right (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

is commensurate with the goal of the application. In other words, the FIPS are applicable once the general structure of the planned system has been established, but they may fail an analyst in understanding whether an application is useful, acceptable to its stakeholders, and commensurate to its perceived or actual privacy impact.

These factors hint at two situations where the FIPS may be difficult to apply. The first is in cases where technology mediates relationships between individuals (i.e., personal privacy, see Section 2.2.2) as opposed to between individuals and organizations. The second is in cases where the data is not structured and application purposes are ill-defined (e.g., exploratory applications).

3.5.1.2 Guidelines for Ubiquitous Computing and Location-Based Services

In addition to general principles, specific guidelines have also been proposed for more limited application domains. For example, Lederer et al. [192] observed that, in the context of ubiquitous computing applications, successful designs must

- make both potential and actual information flows visible,
- provide coarse-grain control,
- enable social nuance, and
- emphasize action over configuration.

These guidelines originate from qualitative reflection on the researchers' experience. Guidelines with even more limited scope are available as well. For example, Iachello et al. proposed eight specific guidelines for the development of social location disclosure applications [153] (Table 3.4).

3.5.1.3 Design Patterns for Privacy

Design patterns are somewhat related to guidelines. The concept of patterns originates from work by Alexander [14], and was later used in the context of software design [111]. One key difference between guidelines and patterns is that patterns are meant to be generative,

Table 3.4 Privacy guidelines for social location disclosure applications and services [153].

Guideline	Description
Flexible replies	Users should be able to choose what the system discloses as a reply to a location request.
Support denial	Communication media should support the ability to ignore requests.
Support simple evasion	Designs should include the ability of signaling "busy" as a baseline evasive reply.
Do not start with automation	Automatic functions that communicate on behalf of the user should not be introduced by default, but only when a real need arises.
Support deception	Communication media should support the ability to deceive in the reply.
Start with person-to-person communication	Social mobile applications should support person-to-person communication before attempting group communication.
Provide status/Away messages	Provide a way of signaling availability status.
Operators should avoid *Handling user data*	Social location disclosure applications should not be provided by centralized services.

helping designers create solutions by re-purposing existing solutions, whereas guidelines tend to be higher level and not tied to specific examples.

Both Junestrand et al. [169] and Chung et al. [55] developed design patterns to solve common privacy problems of ubicomp applications. The patterns developed by Chung et al. are listed in Table 3.5 and are inspired by a combination of the FIPS, HCI research, and security research. While Chung et al.'s patterns are relatively high-level — e.g., "Building Trust and Credibility," "Fair Information Practices," — Junestrand et al.'s are application-specific.

Chung et al. evaluated their patterns using a design exercise with students and experienced designers. The authors observed that the privacy patterns were not used in any meaningful way by the participants. Expert reviewers did not evaluate the designs produced with the patterns to be any better than the others [55]. Several explanations are likely, including limitations of the experimental setup and the fact that privacy is often a secondary concern of the designers.

Table 3.5 Privacy pre-patterns [55].

Design pattern	**Description**
Fair information practices	The fair information practices are a set of privacy guidelines for companies and organizations for managing the personal information of individuals.
Respecting social organizations	If [members of] the organization [. . .] [do] not trust and respect one another, then the more intimate the technology, the more problems there will likely be.
Building trust and credibility	Trust and credibility are the foundation for an ongoing relationship.
Reasonable level of control	Curtains provide a simple form of control for maintaining one's privacy while at home.
Appropriate privacy feedback	Appropriate feedback loops are needed to help ensure people understand what data is being collected and who can see that data.
Privacy-sensitive architectures	Just as the architecture of a building can influence how it is perceived and used, the architecture of a ubiquitous computing system can influence how people's perceptions of privacy, and consequently, how they use the system.
Partial identification	Rather than requiring precise identity, systems could just know that there is "a person" or "a person that has used this system before."
Physical privacy zones	People need places where they feel that they are free from being monitored.
Blurred personal data	[. . .] Users can select the level of location information disclosed to web sites, potentially on a page by page basis.
Limited access to personal data	One way of managing your privacy with others is by limiting who can see what about you.
Invisible mode	Invisible mode is a simple and useful interaction for hiding from all others.
Limited data retention	Sensitive personal information, such as one's location and activity, should only be kept as long as needed and no longer.
Notification on access of personal data	AT&T Wireless' Find Friends service notifies your friend if you ask for her location.
Privacy mirrors	Privacy mirrors provide useful feedback to users by reflecting what the system currently knows about them.
Keeping personal data on personal devices	One way of managing privacy concerns is to store and present personal data on a personal device owned by the user.

The lack of an established design practice and knowledge is an inherent problem with applying design patterns to privacy-sensitive applications. Chung et al. acknowledged that design patterns may be premature in the ubicomp domain. An argument could be made that in situations of exploratory and uncertain design, only thorough analysis on a case-by-case basis can provide strong arguments for an application's acceptability.

3.5.2 Process Frameworks

While guidelines are ready-made parcels of analysis and solutions to common problems, the process frameworks described in this section provide guidance to designers on how to approach the analysis and design of privacy-sensitive IT applications.

3.5.2.1 Questions — Options — Criteria

Media spaces combine audio, video, and computer networking technology to provide a rich communicative environment for collaboration (see Sections 3.1.5 and 3.2.6). Bellotti and Sellen published early work on privacy in the context of video media spaces, based in part on the experience of the RAVE media space at EuroPARC [38].

They developed a framework for addressing personal privacy in media spaces. According to their framework, media spaces should provide appropriate feedback and control structures to users in four areas (Table 3.6). Feedback and control are described by Norman as basic structures in the use of artifacts [222], and are at the base of the Openness and Participation principles in the FIPS.

Bellotti and Sellen adapted MacLean *et al.*'s Questions, Options, Criteria framework [199] to guide their privacy analysis process. They proposed evaluating alternative design options based on eight questions and eleven criteria, derived from their own experience and from other sources (see Table 3.7). Some criteria are closely related to security evaluation (such as trustworthiness), while other criteria try to address the problem of the human cost of security mechanisms. Bellotti and Sellen's criteria are similar to those of Heuristic Evaluation [221], a well-known discount usability technique for evaluating user interfaces.

The evaluation of alternatives is common to several privacy frameworks, and is characteristic of design methods targeted at tough design problems that do not enjoy an established design practice. Bellotti and Sellen do not provide guidance on how to develop design options,

Table 3.6 Questions for video media spaces [38].

Questions	Feedback about	Control over
Capture	When and what information about me gets into the system.	When and when not to give out what information. I can enforce my own preferences for system behaviors with respect to each type of information I convey.
Construction	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviors and permissions.
Accessibility	Which people and what software (e.g., daemons or servers) have access to information about me and what information they see or use.	Who and what has access to what information about me. I can set automatic default behaviors and permissions.
Purposes	What people want information about me for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviors.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

Table 3.7 Evaluation criteria for video media spaces [38].

Evaluation criteria	Description
Trustworthiness	Systems must be technically reliable and instill confidence in users.
Appropriate timing	Feedback should be provided at a time when control is most likely to be required.
Perceptibility	Feedback should be noticeable.
Unobtrusiveness	Feedback should not distract or annoy.
Minimal intrusiveness	Feedback should not involve information which compromises.
Fail-safety	The system should minimise information capture, construction and access by default.
Flexibility	Mechanisms of control over user and system behaviors may need to be tailorable.
Low effort	Design solutions must be lightweight to use.
Meaningfulness	Feedback and control must incorporate meaningful representations.
Learnability	Proposed designs should not require a complex model of how the system works.
Low-cost	Naturally, we wish to keep costs of design solutions down.

acknowledging the complex nature of the design space. However, one could imagine a pattern language such as Chung et al.'s providing such design options.

3.5.2.2 Risk Analysis

Risk management has long been used to prioritize and evaluate risks and to develop effective countermeasures. The use of risk analysis is less common in the HCI and Human Factors communities, although it has been employed to evaluate risks in systems where humans and computers interact, e.g., aviation [217]. However, only recently have risk analysis models been developed in the HCI literature specifically to tackle privacy issues in IT.

Hong et al. proposed using risk analysis to tackle privacy issues in ubicomp applications [146]. Their process enhances standard risk analysis by providing a set of social and technical questions to drive the analysis, as well as a set of heuristics to drive risk management. The analysis questions, shown in Table 3.7, are designed to elicit potential privacy risks for ubicomp applications. The authors propose a semi-quantitative risk evaluation framework, suggesting to act upon each identified risk if the standard "$C < LD$" equation is satisfied.[10] To evaluate the components of this formula, a set of risk management questions are used, listed in Table 3.9.

One important point of Hong et al.'s framework is that it requires the designer to evaluate the motivation and cost of a potential attacker who would misuse personal information. The economic aspect of such misuse is important because it can help in devising a credible risk evaluation strategy and represents the implicit assumption of analysis performed by regulatory entities. Although risk analysis is a fundamental component of security engineering, many aspects of design in this domain cannot be easily framed in a quantitative manner, and a qualitative approach may be necessary. Also, quantitative approaches may prove misleading, failing to consider user perceptions and opinions [45].

[10] C = cost of adequate protection; L = the likelihood that an unwanted disclosure of personal information occurs; D = the damage that happens on such a disclosure.

Table 3.8 Ubicomp privacy risk analysis questions [146].

Social and organizational context

- Who are the users of the system? Who are the data sharers, the people sharing personal information? Who are the data observers, the people that see that personal information?
- What kinds of personal information are shared? Under what circumstances?
- What is the value proposition for sharing personal information?
- What are the relationships between data sharers and data observers? What is the relevant level, nature, and symmetry of trust? What incentives do data observers have to protect data sharers' personal information (or not, as the case may be)?
- Is there the potential for malicious data observers (e.g., spammers and stalkers)? What kinds of personal information are they interested in?
- Are there other stakeholders or third parties that might be directly or indirectly impacted by the system?

Technology

- How is personal information collected? Who has control over the computers and sensors used to collect information?
- How is personal information shared? Is it opt-in or is it opt-out (or do data sharers even have a choice at all)? Do data sharers push personal information to data observers? Or do data observers pull personal information from data sharers?
- How much information is shared? Is it discrete and one-time? Is it continuous?
- What is the quality of the information shared? With respect to space, is the data at the room, building, street, or neighborhood level? With respect to time, is it real-time, or is it several hours or even days old? With respect to identity, is it a specific person, a pseudonym, or anonymous?
- How long is personal data retained? Where is it stored? Who has access to it?

Table 3.9 Risk management questions [146].

Managing privacy risks

- How does the unwanted disclosure take place? Is it an accident (for example, hitting the wrong button)? A misunderstanding (for example, the data sharer thinks they are doing one thing, but the system does another)? A malicious disclosure?
- How much choice, control, and awareness do data sharers have over their personal information? What kinds of control and feedback mechanisms do data sharers have to give them choice, control, and awareness? Are these mechanisms simple and understandable? What is the privacy policy, and how is it communicated to data sharers?
- What are the default settings? Are these defaults useful in preserving one's privacy?
- In what cases is it easier, more important, or more cost-effective to *prevent* unwanted disclosures and abuses? *Detect* disclosures and abuses?
- Are there ways for data sharers to maintain plausible deniability?
- What mechanisms for recourse or recovery are there if there is an unwanted disclosure or an abuse of personal information?

An interesting qualitative approach to risk analysis for ubicomp is provided by Hilty et al. [141]. They suggest using a risk analysis process based on risk screening and risk filtering. In the screening phase, an expert panel identifies relevant risks for a given application (thus using the expert's experience directly, instead of checklists like Hong et al.'s).

In the filtering phase, experts prioritize risks according to several criteria that respond to the *precautionary principle*. According to the precautionary principle, risk management should be "driven by making the social system more adaptive to surprises" [177]. They suggest to filter risks according to qualitative prioritization based on the following criteria [141]:

- Socioeconomic irreversibility (Is it possible to restore the status before the effect of the technology has occurred?)
- Delay effect (is the time span between the technological cause and the negative effect long?)
- Potential conflicts, including voluntariness (Is exposure to the risk voluntary?) and fairness (Are there any externalities?)
- Burden on posterity (Does the technology compromise the possibilities of future generations to meet their needs?)

The authors used this framework to analyze the social and technical risks of ubicomp technologies, including their social and environmental impact. However, while their heuristics are adequate for analyzing large scale social risks, they may not be adequate for risks arising at the interpersonal level. Furthermore, even qualitative risk analysis may be inadequate, because security and privacy design decisions interact with issues that cannot be modeled as risks, both internal (e.g., application usefulness), and external (e.g., regulatory requirements) as pointed out in work by Hudson and Smith [148] and Barkhuus and Dey [30].

3.5.2.3 Functionality- and Goal-Oriented Analysis

One of the difficulties in identifying privacy requirements is that they are often non-functional characteristics of a product and are difficult to enumerate exhaustively. Patrick and Kenny's Privacy Interface Analysis (PIA) is a process to systematically identify vulnerabilities in privacy-sensitive user interfaces [230]. In PIA, designers describe the service or application using UML case models and derive the necessary interface functionalities from them. Then, they consider each functionality with respect to the principles of *transparency*, *finality and use limitation*, *legitimate processing*, and *legal rights*. Patrick and Kenny combine a functionality-oriented analysis process with an evaluation of the legal and social legitimacy of a given application. However, their process is relatively time consuming.

STRAP (Structured Analysis Framework for Privacy) also attempts to facilitate the identification of privacy vulnerabilities in interactive applications [163]. STRAP employs a goal-oriented, iterative analysis process, and is composed of three successive steps: vulnerability analysis, design refinement, and evaluation. The analyst starts by defining the overall goals of the application and recursively subdividing these goals into subgoals in a tree-like fashion. Specific implementations are then attached to the leafs of this recursive goal definition tree, and vulnerabilities are then identified for each, leading to privacy requirements.

Jensen compared STRAP's performance with PIA's [230], Bellotti and Sellen's framework [38], and Hong's Risk Analysis framework [146]. The results of this evaluation encouragingly suggest that designers using STRAP identified more privacy issues and more quickly than the other groups. Jensen notes, however, that the design of a shared calendaring system used in the study did not overlap with the applicability domain of the frameworks developed by Bellotti and Sellen and by Hong et al. This underscores the importance of tightly defining the scope of design methods.

3.5.2.4 Proportionality

Iachello and Abowd proposed employing the principle of proportionality and a related development process adapted from the legal and Data Protection Authority communities to analyze privacy [152]. In a nutshell, the proportionality principle asserts that the burden on stakeholders of any IT application should be legitimate, i.e. compatible with the benefits of the application. Assessing legitimacy implies a balancing between the benefits of data collection and the interest of the data subject in controlling the collection and disclosure of personal information. This balancing of interests is employed by the European data protection community and in the United States, by the Supreme Court [278].

Iachello and Abowd further propose to evaluate design alternatives at three stages of an iterative development process: at the outset of design, when application goals are defined (this part of the analysis is called the "desirability" judgment); during the selection of a technology to implement the application goals (this part is called "appropriateness"); and during the definition of "local" design choices impacting parameters and minor aspects of the design (this part is called "adequacy").

Iachello and Abowd evaluated the proportionality method in a controlled experiment with Hong's risk analysis [146], Bellotti and Sellen's method [38], and, as a control condition, Design Rationale [200]. The results of the evaluation show that none of the participants in the four conditions identified all the privacy issues in the application. Each design method prompted the participants of the evaluation to probe a certain set of issues, based on the questions that were included in the design framework. Moreover, the level of experience of the participants and the amount of time employed to perform the analysis were better correlated than the design method used with the number of privacy issues identified by each participant [151].

The results of this study suggest that, again, the scope of the design method strongly influences its effectiveness in analyzing specific design problems. Second generation design methods [99] can help in the privacy requirements analysis by forcing designers to think through the design as extensively as possible.

3.5.3 Modeling Frameworks

The third type of "design methods" we discuss are modeling frameworks. Some modeling frameworks, such as k-anonymity [274] and the Freiburg Privacy Diamond [314], are heavily influenced by information theory. They describe exchanges of information mathematically, which allows for requirements to be tightly defined and verified. Given the lack of reference to the human user, however, these frameworks are not used in the HCI community. Instead, HCI researchers have focused on economic and behavioral models.

3.5.3.1 Economic Frameworks and Decision-Making Models

Researchers have developed economic models to describe individuals' decision making in the disclosure of personal information. Early work in this area includes Posner's and Stigler's work in the late 1970s [235, 271]. In particular, Posner argues that privacy is detrimental from an economic standpoint because it reduces the fluidity of information and thus market efficiency.

Posner predicts markets for personal information, where individuals can freely trade their personal data. Varian argues that from an economic analysis standpoint, personal information could be protected by associating with it an economic value, thus increasing the cost of collecting and using it to an equitable balance [288]. In these markets, data users pay license rights to the data subjects for using their personal information. Similar markets exist already (i.e., credit and consumer reporting agencies). However, critics of these economic models question whether increased fluidity actually provides economic benefit [212]. It should be noted that these markets are quite incompatible with the underlying assumptions of data protection legislation such as EU Directive 95/46, which treats personal information as an unalienable object and not as property.

Varian takes a more pragmatic approach, suggesting that disclosure decisions should be made by balancing the costs and the subjective benefits of the disclosure [288]. Researchers have also developed economic models to describe disclosure behaviors. For example, Vila et al. have developed a sophisticated economic model to explain the low effectiveness of privacy policies on web sites [291]. Acquisti explains why Privacy-Enhancing Technologies (PETs) have not enjoyed widespread adoption, by modeling the costs and expected benefits of using a PET versus not using it, treating users as rational economic agents [7]. Acquisti also argues that economics can help the design of privacy in IT by identifying situations in which all economic actors have incentives to "participate" in the system (e.g., in systems that require the collaboration of multiple parties, such as anonymizing networks). He further contends that economics can help in identifying what information should be protected and what should not, for example, by identifying situations in which the cost of breaching privacy is lower than the expected return (a basic risk analysis exercise).

The main limitation of economic models is that the models' assumptions are not always verified. Individuals are not resource-unlimited (they lack sufficient information for making rational decisions), and decisions are often affected by non-rational factors such as peer pressure and social navigation [8]. One explanatory theory Acquisti and Großklags discuss is that of *bounded rationality*, i.e., that individuals cannot fully process the complex set of risk assessments, economic constraints, and consequences of a disclosure of personal data.

Acquisti and Großklags' research casts serious doubts on whether individuals are capable of expressing meaningful preferences in relation to data protection. While in interpersonal relations, individuals have a refined set of expectations and norms that help decision-making and a fine-grained disclosure or hiding process, the same is not true for data protection disclosures.

The Approximate Information Flows (AIF) framework proposed by Jiang et al. [168] combines ideas from economics and information theory. In AIF, Jiang et al. state the Principle of Minimum Asymmetry:

> *"A privacy-aware system should minimize the asymmetry of information between data owners and data collectors and data users, by decreasing the flow of information from data owners to data collectors and users and increasing the [reverse] flow of information... "* [168]

To implement this principle, the authors propose a three-pronged strategy. First, personal information should be managed by modulating and enforcing limits on the persistency (retention time), accuracy (a measure of how precise the data is), and confidence (a probability measure that the data is correct) of information within an information system. Second, the personal information lifecycle should be analyzed according to the categories of collection, access, and second use. Third, at each of these stages, the system should provide ways to prevent, avoid, and detect the collection, access and further use of personal information.

The authors used AIF to analyze several technologies and applications, such as P3P, and feedback and control systems, to show how these fit within the framework. However, this model has some limitations. First, the authors have used AIF as an analytic tool, but it has not been used as a design model. Second, all data users are expected to comply with the AIF model and respect the constraints on the use and interpretation of personal data. Finally, there is a potential conflict between this approach and data protection legislation in certain jurisdictions, because data protection legislation requires data controllers to guarantee the integrity and correctness of the data they are entrusted with, which is incompatible with the idea of data "decay" proposed by the AIF framework.

3.5.3.2 Analytic Frameworks

Analytic frameworks attempt to answer the question "what is privacy" in a way that is actionable for design purposes. For example, Multilateral Security is an analysis model for systems with multiple competing security and privacy requirements [210, 242]. One of the innovations of Multilateral Security is that it frames privacy requirements as a special case of security requirements. According to Multilateral Security, security and privacy are elements of the same balancing process among contrasting interests. The aim is to develop technology that is both acceptable to users and profitable for manufacturers and service providers. Multilateral Security asserts that designers must account for all stakeholders' needs and concerns by

— considering and negotiating conflicting requirements,
— respecting individual interests, and
— supporting user sovereignty.

Consequently, Multilateral Security highlights the role of designers in producing equitable technology, and that of users who must be “empowered” to set their own security or privacy goals [310]. Multilateral security was applied to several case studies, including a deployment of a prototype mobile application for “reachability” management for medical professionals (i.e., brokering availability to incoming phone calls) [243].

A different model is offered by Lederer et al.’s deconstruction of the privacy space [193]. According to Lederer et al., privacy issues can be classified along six dimensions (Table 3.10). These dimensions are obtained from the analysis of prior literature, including Agre [11], Lessig [195], and Agre and Rotenberg [12]. Privacy issues located in different positions of the space will have different characteristics and typical design solutions will be different. Unfortunately, Lederer et al. do not describe what design solutions should be used for applications in various locations of this analytical space. Thus, Lederer et al.’s framework is a good candidate for a privacy vocabulary and as a descriptive model, but currently does not necessarily help as an aid to design.

In addition to general models, constrained models exist for specific applications. Adams presents a model to analyze perceived infringe-

Table 3.10 Privacy dimensions [193].

Dimension	Description
Feedback and control	Different privacy-related systems employ different ratios, degrees, and methods of feedback about and control over the disclosure process.
Surveillance vs. Transaction	Surveillance relates to continuous observation and collection of personal information (e.g., surveillance cameras). Transactions are identifiable events in which personal information is exchanged (e.g., purchase on the internet).
Interpersonal vs. Institutional	Distinction between revealing sensitive information to another person and revealing it to industry or the state. Similar to our distinction of personal privacy and data protection in Section 2.2.2, limited to the recipient of personal information.
Familiarity	The degree of acquaintance of the recipient to the disclosing party and vice-versa.
Persona vs. Activity	Whether the information relates describes the individual (e.g., age, address) or her actions (e.g., crossing an automatic toll booth).
Primary vs. Incidental	Here we distinguish between whether the sensitive information is the primary content or an incidental byproduct of the disclosure.

ments of privacy in multimedia communication systems [9]. Through several user evaluations, she identified three factors that influence people's perceptions of these systems: information sensitivity, i.e., how private a user considered a piece of information; information receiver, i.e., who the person receiving the information was; and information usage, i.e., how the information will be used.

Boyle and Greenberg define a language for privacy in video media spaces, i.e., networked teleconferencing and awareness applications using digital video and audio feeds. Boyle and Greenberg provide a comprehensive summary of research on privacy in media spaces [45]. They claim that in these applications, designers must consider at least the following privacy issues:

- Deliberate privacy abuses.
- Inadvertent privacy violations.
- Users' and nonusers' apprehensiveness about technology.

Boyle and Greenberg also propose deconstructing the far-reaching concept of privacy into three aspects: solitude ("control over one's interpersonal interactions," akin our definition personal privacy), confidentiality ("control over other's access to information about oneself," i.e., informational self-determination), and autonomy ("control over the observable manifestations of the self," also related to a concept of personal privacy).[11] However, Boyle and Greenberg observe that that there is still insufficient knowledge about the users of this technology to draft effective guidelines. Even worse, the authors note that the very analytic tools currently employed are still inadequate for mapping system functions (e.g. "open a communication channel") to individual preferences and actions.

3.5.3.3 Conclusions on Modeling Frameworks

Patterns and guidelines are similar in many respects because they provide a standard set of typical solutions to the designer and are popular due to their relatively simple structure and ease-of-use. For

[11] Quotes from Boyle and Greenberg [45].

well-established domains and technologies these can be very useful. However, it becomes very difficult to apply them when the scope and level of generality of the guideline do not match with the design task.

Process methods standardize the analysis and design process, and increase the coverage of the design space by considering as many questions and issues as possible upfront. The proponents of modeling frameworks attempt to proceed one step further, by systematizing factual knowledge about privacy in general structures that can be used for many types of applications. However, experimental evidence and our review of the literature suggest that the privacy design space may be too broad to be systematized in one single framework or model. If different methods address different parts of the design space, one option for attempting to increase analytic and design thoroughness would be to combine methods.

While this is indeed possible, we believe that a combined method would be even more difficult to validate and would not be adopted easily. An alternative to creating a large unified analysis process would be to document a modular toolbox of privacy heuristics that can be used upon need with a clear understanding of their limitations and contributions. This *privacy toolbox* should clearly indicate for what applications and social settings certain approaches are more effective, and what the designer can expect from them. We will return to this subject in Section 4.3.

4

Trends and Challenges in Privacy HCI Research

In the previous chapters, we provided an overview of the research landscape of HCI as it relates to privacy. As a conclusion to this article, we outline several trends that are changing the privacy landscape, as well as major research challenges in the field. While the research subfields reviewed in Chapter 3 tackle a specific aspect of privacy in HCI, we focus here on five "grand challenges" that span several subfields:

- Developing more effective and efficient ways for end-users to manage their privacy.
- Gaining a deeper understanding of people's attitudes and behaviors toward privacy.
- Developing a "Privacy Toolbox."
- Improving organizational management of personal data.
- Reconciling privacy research with technological adoption models.

Below, we outline each of these trends, indicate where we see current research headed, and what are the challenges facing researchers and practitioners.

4.1 Better Ways of Helping End-Users Manage Their Personal Privacy

It is becoming increasingly difficult to manage personal privacy as information and communication technologies become pervasive. Personal information is fragmented across a number of devices, applications, web sites, and organizations, each with different user interfaces, notifications, and management policies. We argue that we need new approaches for alleviating the burden of managing users' personal privacy.

Information and communication technologies increasingly preserve information about the individuals using them[1] and surveillance systems are spreading into the workplace (in the form of email and web monitoring) and to other spheres of daily activity (e.g., broadcasting the interior of night clubs, bars, or beaches [47]). Often, these systems collect information unbeknownst to the user. Furthermore, the development of digital sensors has enabled the collection of novel types of information in everyday situations (e.g., automatic toll payment systems based on RFID and license plate recognition [107], implantable sensors monitoring the health of patients [201], monitoring systems deployed in the homes of elderly people [33]). Technical and economic considerations suggest that sensing technologies will become a ubiquitously present infrastructure, open for use by individuals as well as organizations for a wide array of purposes. A distinctive characteristic of these systems is that the interaction is increasingly becoming implicit, out of the scope of control of Norman's "Seven Steps of Interaction" [222]. This kind of implicit interaction requires new mechanisms for managing the resulting risks to personal information and privacy.

One possible solution to the problems above is to develop more effective and less burdensome user interfaces for helping people make good decisions. A key challenge here is that there is currently no agreement as to what kinds of interaction styles are best for each type of information disclosure. Rule- or policy-based mechanisms may be sub-

[1] For example, personal video recorders capture a person's television viewing habits, mobile phones contain photos, call history, instant messages, and contacts, etc.

optimal for many applications, as discussed in Section 3.2.2. Other interaction styles, such as social translucency and plausible deniability, might be able to achieve comparable effects with far less burden and with a greater sense of control [22], but there are no clear guidelines on how to build plausible deniability into computing systems. Ambiguity has been discussed as a design resource in other contexts (e.g., games) [113], and we believe it will become an increasingly important design element in the context of privacy. In short, there needs to be much more work to determine the efficacy of these different ideas in a wider range of contexts.

Another possibility is to consider a better division of labor that helps shoulder the burden of managing personal privacy. A consensus is slowly building in the research community that privacy-sensitive applications cannot make all data transfers explicit, nor require users to track them all. The related UIs and interaction patterns would simply be too complex and unwieldy. From a data protection viewpoint, experience shows that most data subjects are unable or unwilling to control all disclosures of personal information, and to keep track of all parties that process their personal data [58, 91]. Distributing the burden of managing one's personal privacy across a combination of operating systems, networking infrastructure, software applications, system administrators, organizations, and third parties could help address this problem. Ideally, these entities would provide advice to users or make trusted decisions on their behalf, with the ultimate goal being to reduce the overall effort required to make good decisions. Taking email spam as an example, multiple entities — including ISPs, local system administrators, and automatic filters — all contribute to reducing the amount of spam that end-users receive. Here, it makes sense to share the costs of spam reduction since the hardship would otherwise be borne by a large number of individuals.

Trusted proxies are another example of a third-party organization that can help manage privacy. For instance, MedicAlert is a paid service that stores personal medical records and forwards them to first responders in the case of medical emergencies. Such organizations, either not-for-profit (like MedicAlert), or for-profit (regulated by a service contract), could include:

- Evaluation clearinghouses, that indicate what products and services to trust. For example, SiteAdvisor [260] evaluates web sites' spam, popup, and virus risks, and provides ratings via a web browser plug-in.
- Services that hold users' location information and disclose it in case of emergency or subpoena, similar to current mobile telecom operators.
- A service that seeds suspected privacy violators with fake personal data and tracks how that data is used and shared.
- A service that checks if an individual reveals too much personal information online and is at risk for identity theft [275].

In summary, privacy protection is a "systemic property" that requires support at all levels. However, special care should be exercised in allocating responsibility and oversight correctly, because the business goals of many organizations may not be aligned with those of the users, as suggested by recent controversies over security leaks at large personal data brokerage firms [295, 298].

4.2 A Deeper Understanding of People's Attitudes and Behaviors toward Privacy

The second challenge is in gaining a deeper understanding of the behaviors of individuals toward privacy-affecting systems, at all levels of interaction.

One area where research is needed is better understanding of users' behavior with warnings and notifications. There are many difficult forces to balance in creating an effective warning system. Warnings must be visible, comprehensible, understandable, and plausible to end-users [64, 309]. Cranor has also argued that warnings need to be tied to clear actions,[2] and be designed so that users keep doing the right thing (rather than ignoring or turning them off). A counterexample to almost all of the above would be standard warning dialogs, most of which are simply dismissed because they get in the way of the user's primary goals.

[2] Echoing the UI design advice in Section 3.2: "Present choices, not dilemmas."

A second needed line of research is in understanding how attitudes and behaviors toward privacy-affecting systems evolve and reconcile over time. For example, recent research has shown that behavior in privacy matters often differs from stated preferences, for a variety of reasons [267]. Acquisti and Gross have even shown that on the Facebook social networking site, people perceived others as revealing too much information despite revealing a great deal of information about themselves [128].

A third needed line of work is that of understanding how to influence the behavior of users. For example, Jagatic et al. provide a striking instance of how publicly available information gathered from social networking web sites can be used to trick people into giving up personal information, such as passwords. They showed that individuals are more likely to fall for phishing attacks if the sender is from their existing social network [160]. These attacks are known as *spear-phishing*, or *context-aware phishing*. By incorporating sender information mined from a social networking site, they showed that scam emails were much more effective in deceiving the targets. Two other examples of research that would fall into this category include convincing people not to abuse other people's trust (for example, cyber-stalking a person), and persuading people that they can do simple things to protect their privacy online.

Here, one challenge is that the very behaviors under scrutiny are not stable, but evolve with the adoption of new technologies. For example, the surge of identity theft and the enactment of legislation countering it suggests that the public is becoming slowly, if painfully, aware of the risks of combining personal information from multiple data sources. On the other hand, the availability of personal information from multiple sources has transformed the previously difficult task of constructing individuals' profiles into a fairly trivial activity [227]. It is not uncommon for people to "google" potential dates and prospective employees and find past postings on message boards, photographs, and with some effort, information on political affiliations, social networks, criminal records, and financial standing.

Furthermore, the willingness of people to ultimately accept these technologies despite the intrinsic risks shows that HCI researchers should not trust stated preferences relative to unknown technologies, but analyze the use of the technologies in practice. We discuss this point further below in Section 4.5 in relation to acceptance.

To summarize, we see an increasing role for "behavioral" research in HCI relative to privacy. The cost of this kind of research is higher than traditional survey-based or even lab-based experiments. However, we are convinced that the nature of the issues revolving around privacy demand this additional expense if the goal is to obtain credible and generalizable results.

4.3 Developing a "Privacy HCI Toolbox"

A third "grand challenge" is providing more support to guide the development of privacy-sensitive systems. Design teams often have to grope through a design space, relying primarily on their intuition to guide them. What is needed are better methods, tools, guidelines, and design patterns to help teams iteratively design, implement, and evaluate applications.

With respect to design, we believe that there would be great value in developing an organic *privacy toolbox.* This privacy toolbox would be a catalog of privacy design methods and models, with an indication of the applications and social settings each can be applied to. Practitioners could then choose to use these tools with a full understanding of their contributions and limitation. We would like to stress that we are not proposing to develop a Software Engineering "methodology" [265] — our proposal is simply a coherent collection that assists practitioners.

An initial catalog of design techniques for privacy and HCI would be relatively easy to devise. For example, we mentioned above that the FIPS are particularly fit for large personal data processing enterprises and have been adapted to novel technologies, both in the technical literature [112, 186] and in the Data Protection Authority community. Similarly, privacy guidelines, patterns, and risk models could help designers in specific, well delimited, circumstances [55, 152, 230].

A precise description of method applicability is essential. Thus, the toolbox should include a selection process, based on criteria including the application domain, the deployment context, and the type of privacy and security issues involved (e.g., personal privacy, data protection, sensitive information, etc.). A credible selection process requires the testing of the various methods' effectiveness and usefulness, which is by far the most challenging aspect of this idea.

With respect to implementation, design teams are sorely lacking tools, frameworks, and reusable UI components and metaphors for creating privacy-sensitive systems. Examining the evolution of the graphical user interface (GUI) may help chart a research agenda to address this need. Similar to GUI components, we could develop reusable privacy tools, services, and toolkits for building privacy-sensitive UIs. Some possibilities include specialized GUI widgets and interaction techniques for helping end-users manage their personal privacy, new visualizations and user interfaces for helping administrators set privacy policies and manage large collections of personal information, and model-based user interfaces for weaving and enforcing privacy throughout the entire UI.

Developers should also pay attention to seemingly innocuous technologies that may have unintentionally negative privacy implications (e.g., cookies in web browsers). Verification techniques able to identify these issues upfront, before deployment, would be very beneficial. However, the unpredictable nature of emergent use suggests that systematic techniques for identifying these issues may be very difficult to devise.

Finally, regarding evaluation, design teams need techniques specific to privacy, similar to heuristic evaluation and cognitive walkthrough. There is a general lack of understanding on how to evaluate the quality of a design with respect to privacy. This challenge is exacerbated by the rarity of documented privacy breaches, by the disconnect between the time and place of the actual privacy breach and when the user becomes aware of it, and by the ever-shifting attitudes and behaviors of users becoming familiar with new technologies.

Several techniques have been employed to address these challenges, such as presenting realistic previews of features (e.g., with the scenarios discussed in Section 3.1.6), sampling people's reactions to privacy concerns through remote usability tests and remote surveys, etc. Some work has also been already done on adapting QOC and heuristic evaluation (e.g., Bellotti and Sellen's QOC technique [37]). Other promising, yet unexplored, approaches are the use of cognitive walkthroughs tailored for privacy, as well as improved methods for conducting user studies to elicit possible privacy concerns. However, work on validating these techniques to assess their effectiveness is necessary before practitioners will be willing to embrace them.

4.4 Better Organizational Practices

The fourth research challenge encompasses the development of tools for managing personal information within organizations.

Several authors have pointed out that information security software often fails not due to technical causes, but because of issues of management and control of the people operating the technology [208, 255]. In his study of Automatic Teller Machines (ATM) failures, Anderson indicated that the three main reasons for failure were program bugs, interception of mail containing ATM cards, and theft and fraud by insiders [19]. Similarly, reports of privacy breaches show that many breaches are attributable to those responsible for safeguarding the data, for example, airlines providing data to third parties [20], or consumer reporting agencies providing personal data to outsiders pretending to be legitimate customers [295].

The privacy breaches mentioned above indicate that helping organizations create and enforce effective privacy policies is a significant research challenge that should also involve researchers both in HCI and CSCW. Corporate caretakers of personal information are becoming increasingly aware of the importance of privacy. Many companies have defined policies and procedures for handling personal information, and a few have gone so far as creating the position of Chief Privacy Officer. Some of these programs have been enacted voluntarily, under pressure by the market to curb privacy breaches. Other organizations have implemented these changes to comply with legislation such as EU Directive 95/46 or HIPAA.

Knowledge in this area is in part hidden behind corporate walls, and the academic community has largely ignored these issues. This lack of attention in academia is worrying, because management of personal information is one of the most challenging aspects of IT security today [178]. Much more work is needed in this domain, and specifically in three areas: (1) defining privacy policies, (2) implementing and enforcing them, and (3) auditing system performance.

With respect to the first issue, we need better tools for defining privacy policies, both at the level of the organization and in relation to its IT systems. Industry standards and procedures could be very helpful to draft policies [150], but require an open dialogue between industry and academia with which many commercial organizations may still be uncomfortable. Once policies are drafted, tools such as IBM's SPARCLE [172] could be used to convert the policies into machine-readable form, facilitating implementation. One fundamental open question is whether a machine-readable privacy policy language (e.g., P3P) can be comprehensive enough to model all possible requirements and organizational assumptions.

Second, we need more support for implementing and enforcing privacy policies. These challenges rest both with the people and the technology involved in the personal data processing. The technical implementation of privacy policies has been the topic of systems research [24], and some of those ideas have been incorporated into commercial products (e.g., IBM's Tivoli product line). It is worth noting that the challenge of enforcement is exacerbated as we move toward mobile and ubiquitous computing environments. A single, unaccounted mobile device can create massive problems for an organization that are difficult to remedy. For example, because most laptops are configured to tunnel through corporate firewalls, a company would have to assume that a lost or stolen laptop could be used to breach network security. There have also been many incidents of laptops containing personal data on thousands of people being stolen or lost. Incidents like these dramatically expose organizations' vulnerability to large-scale identity theft.

Technical considerations aside [42, 240], there are also considerable acceptance challenges to implementing a privacy management program within an organization. Developing the "human" side of the policies should be a priority for the MIS and CSCW communities, as shown by the work by Adams and Blandford. Adams and Blandford discuss the effects of the introduction of access control systems to patient data within a health care settings [10]. They studied two hospitals through in-depth interviews, focus groups, and observations, and found that in one hospital, a user-centered approach resulted in a collaborative system that was accepted and used by the organization, but still clashed with existing working practices. In the second hospital, poor communication to workers about IT security resulted in their misuse by some employees, who viewed them as a tool of social control. Similarly Gaw et al. observed that email encryption tools can fail adoption because of social pressure and perceptions of one's identity [115].

Finally, the privacy community needs better tools for performing audits, probing data processing practices, and tracing information leaks. The former tools would ensure that information is not being leaked accidentally (e.g., being published on web sites, such as in a case with AOL [167]) or intentionally. The latter tools would ensure that any published information can be traced back to the original owner so that appropriate corrective actions can be taken.

Sasse reflects on the current "usability disaster" afflicting security technology and suggests two courses of action for recovery [250]. She suggests using HCI techniques to analyze the cognitive demands of security technologies such as password schemes. Sasse also suggests using these techniques to predict expected behaviors, such as users writing down hard-to-remember passwords. In fact, Sasse points out relevant research challenges, noting that carelessness for security and privacy depends largely on user attitudes. One possible way of fostering secure behavior is to make it the preferable option, that is devising technologies that are secure *by default*. We took a similar stance above in Section 3.3.3, when we discussed the option of motivating users to adopt more secure behaviors.

In summary, since HCI researchers have started to study how security technology is used in the real world [82], security and privacy management should be viewed as a major and promising item requiring much additional research.

4.5 Understanding Adoption

Finally, the fifth emerging theme that we see emerging is the convergence of research on privacy with research on end-user technological acceptance and adoption. The main evidence supporting this trend is (1) that privacy expectations and perceptions change over time as people become accustomed to using a particular technology, and (2) that privacy concerns are only one of several elements involved in the success of a particular application.

In Section 3.1, we described some methods that have been employed to understand user needs; however, it is still difficult to assess what the potential privacy impact will be before actually deploying a system. A typical process is to develop a full system (or new feature), deploy it, and then wait for negative responses from the public or the media, fixing or canceling the system in response.[3] However, it is well known that modifying an existing system late in the design cycle is an expensive proposition. There is a strong need for better methods and tools for quickly and accurately assessing potential privacy risks as well as end-user privacy perceptions. To illustrate this argument, we consider the acceptance history of ubiquitous computing technologies, which have been hotly debated for the past 15 years over their effects on privacy.

[3] Part of the reason for this casual approach is that many developers do not expect such negative reactions from their work. For example, in September 2006, Facebook, a social networking site targeted at college students, added two new features to their site, News Feed, and Mini-Feed [175]. News Feed was a content module that showed what recent changes had occurred with friends and when. For example, News Feed would show that a friend had joined a group recently or had added another person as a friend. Similarly, Mini-Feed lets others see what recent changes an individual had made to their profile. What is interesting is that, although all of this information was already publicly available through a person's Facebook profile, these features generated a tremendous amount of resentment from Facebook users, over concerns of being stalked and a lack of appropriate privacy controls in one's joining or leaving a certain social group.

Facebook's experience is far from exceptional. Many other projects have faced similar concerns. For example, in 1990, Lotus proposed to sell a Housing Marketplace CD which provided directory information on the buying habits of 120 million people in the United States [13]. That project was canceled due to privacy concerns. In 1999, Intel proposed to add unique IDs to each of their processors, to facilitate asset management and provide hardware-based certificates [203]. Intel quickly reverted to disabling this feature by default.

4.5.1 A Story of Rejection And Acceptance: The Importance Of Value Propositions

Xerox PARC's initial foray into ubiquitous computing in the late 1980's provides an instructive case study on privacy. While groundbreaking research was being conducted at PARC, researchers in other labs (and even at PARC) had visceral and highly negative responses to the entire research program. Harper quotes one colleague external to the research team which developed Active Badges as saying:

> *"Do I wear badges? No way. I am completely against wearing badges. I don't want management to know where I am. No. I think the people who made them should be taken out and shot... it is stupid to think that they should research badges because it is technologically interesting. They (badges) will be used to track me around. They will be used to track me around in my private life. They make me furious."* [137]

The media amplified the potential privacy risks posed by these technologies, publishing headlines such as "Big Brother, Pinned to Your Chest" [62] and "Orwellian Dream Come True: A Badge That Pinpoints You" [261]. Ubiquitous computing was not seen as an aid for people in their everyday lives, but as a pervasive surveillance system that would further cement existing power structures. Similar observations were voiced also in the IT community. For example, Stephen Doheny-Farina published an essay entitled "Default = Offline, or Why Ubicomp Scares Me" [80]. Howard Rheingold observed that ubiquitous computing technologies "might lead directly to a future of safe, efficient, soulless, and merciless universal surveillance" [244].

One reason for these negative reactions was that PARC's ubicomp system was "all or nothing." Users did not have control on how the information was shared with others. There were no provisions for ambiguity. Furthermore, the system provided no feedback about what information was revealed to others. This resulted in concerns that a co-worker or boss could monitor a user's location by making repeated queries about the user's location without that user ever knowing.

A second important reason for these reactions lays in the way the ubiquitous computing project itself was presented. The researchers often talked about the technological underpinnings, but had few compelling applications to describe. Thus, discussions often revolved around the technology rather than the value proposition for end-users. To underscore this point, once researchers at PARC started talking about their technology in terms of "invisible computing" and "calm computing," news articles came out with more positive headlines like "Visionaries See Invisible Computing" [248] and "Here, There, and Everywhere" [297].

Thinking about privacy from the perspective of the value proposition also helps to explain many of the recent protests against the proposed deployment of Radio Frequency Identification (RFID) systems in the United States and in England [32]. From a retailer's perspective, RFIDs reduce the costs of tracking inventory, and maintaining steady supply chains. However, from a customer's perspective, RFIDs are potentially harmful, because they expose customers to the risk of surreptitious tracking without any benefit to them.

4.5.2 Models of Privacy Factors Affecting Acceptance

The lack of a value proposition in the privacy debate can be analyzed using "Grudin's Law." Informally, it states that when those who benefit from a technology are not the same as those who bear the brunt of operating it, then it is likely to fail or be subverted [129]. The privacy corollary is that when those who share personal information do not benefit in proportion to the perceived risks, the technology is likely to fail.

However, a more nuanced view suggests that even strong value proposition may not be sufficient to achieve acceptance of novel applications. Eventually, applications enter the hands of users and are accepted or rejected based on their actual or perceived benefits. HCI practitioners would benefit from reliable models of how privacy attitudes impact adoption. We see two aspects of understanding acceptance patterns: (1) a "static" view, in which an acceptance decision is made one-off based on available information, and (2) a dynamic view, in which acceptance and adoption evolve over time. We discuss two working hypotheses of these acceptance models next.

4.5.2.1 Static Acceptance Models

In a renowned article on technology credibility, Fogg and Tseng drafted three models of credibility evaluation: the binary, threshold, and the spectral evaluation models [106]. Fogg and Tseng argued that these models helped explain how different levels of interest and knowledge affect how users perceive the credibility of a product, thus impacting adoption. We advance a similar argument here, adopting these three models with respect to privacy (see Figure 4.1).

The *binary evaluation model* suggests that the acceptance or rejection of a technology is impacted by its perception of being trustworthy (or not) in protecting the user's privacy. This strategy is adopted by users who lack the time, interest, or knowledge for making a more nuanced decision.

The *threshold evaluation model* is adopted by users with moderate interest or knowledge in a particular technology. It suggests that a product is accepted if the perceived trustworthiness is above a certain threshold. Between these thresholds, a more nuanced opinion is formed by the user and other considerations are brought to bear, which may affect an acceptance judgment.

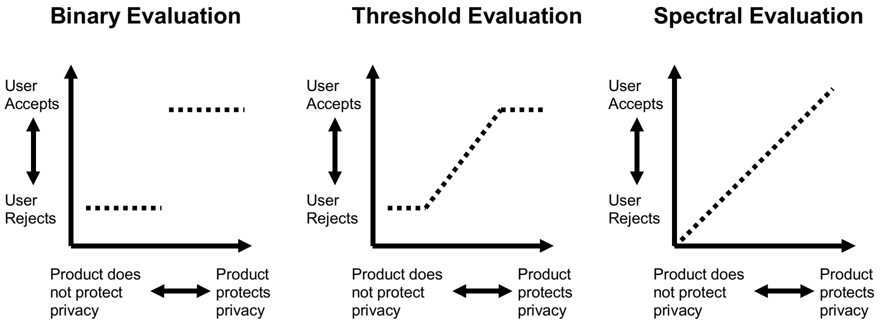


Fig. 4.1 Three models of privacy concerns impacting adoption. A simple view of the domain leads to a binary evaluation model. Increasingly sophisticated understanding allow users to employ more refined evaluation models (Threshold Evaluation and Spectral Evaluation). Picture adapted from Fogg and Tseng [106].

The *spectral evaluation model* is adopted by users with the resources and knowledge to form a sophisticated view of a system, and does not necessarily imply a flat-out rejection or acceptance of a system, whatever its privacy qualities.

While these models are only informed speculation, we believe that there is value in studying acceptance in the context of HCI and privacy. MIS literature on technological acceptance informs us that adoption hinges on several factors, including usability, usefulness, and social influences. Social influences also includes social appropriateness and the user's comfort level, specifically in relation to privacy concerns [290].

Patrick, Briggs, and Marsh emphasize the issue of trust as an important factor in people's acceptance of systems [229]. They provide an overview of different layered kinds of trust. These include dispositional trust, based on one's personality; learned trust, based on one's personal experiences; and situational trust, based on one's current circumstances. They also outline a number of models of trust, which take into account factors such as familiarity, willingness to transact, customer loyalty, uncertainty, credibility, and ease of use. There currently is not a great deal of work examining trust with respect to privacy, but the reader should be convinced that there is a strong link between trust and privacy.

One complication of these theories is that the cultural context affects acceptance. Themes that are hotly debated by a nation's media can significantly impact the perception of privacy risks. For example, a 2003 poll in the European Union showed that privacy concerns vary by national context based on media attention on the subject [98]. However, it is not clear how to reliably predict such concerns when moving from country to country. Perhaps a general survey administered prior to deployment could be useful in these situations. Finally, other factors, such as education, socio-economic status, and labor relations can affect privacy concerns, but we are not aware of any work in these areas in the HCI community. Clearly, there needs to be more work focusing on cultural and social context to gain a more refined understanding of how the phenomena of acceptance unfolds within a given user base.

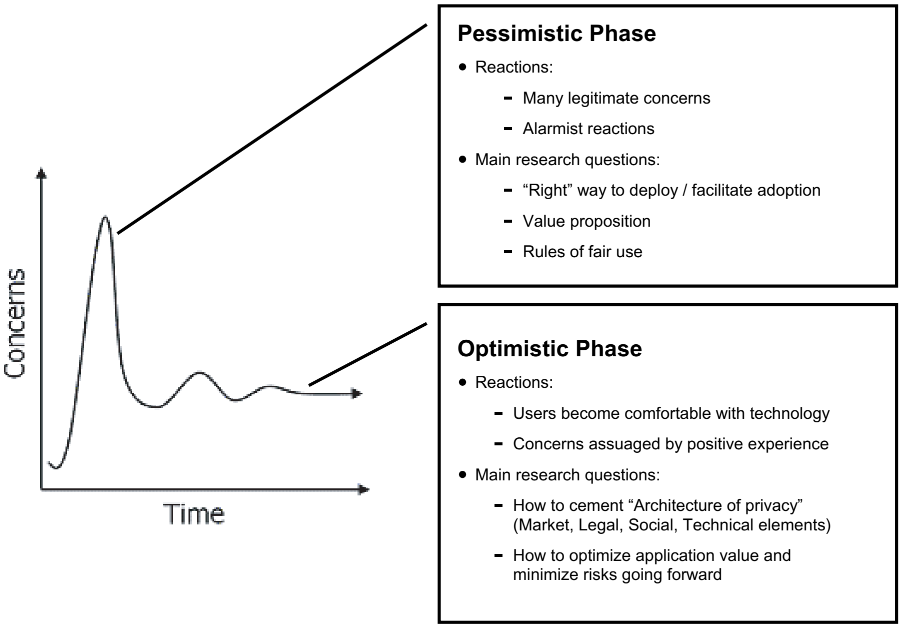
4.5.2.2 The Privacy Hump

In addition to static acceptance models, HCI practitioners would benefit from reliable models to predict the *evolution of privacy attitudes and behaviors over time* [154]. Looking back at past technologies and understanding the drivers for acceptance or rejection can help formulate informed hypotheses going forward.

Our basic assumption is that the notion of information privacy is constantly re-formulated as new technologies become widespread and accepted in everyday practice. Some technologies, initially perceived as intrusive, are now commonplace and even seen as desirable, clearly demonstrating that peoples' attitudes and behaviors toward a technology change over time. For example, when the telephone was first introduced, many people objected to having phones in their homes because it "permitted intrusion... by solicitors, purveyors of inferior music, eavesdropping operators, and even wire-transmitted germs" [102]. These concerns, expressed by people at the time, would be easily dismissed today.

We hypothesize that the resistance in accepting many potentially intrusive technologies follows a curve that we call "the Privacy Hump" (see Figure 4.2). Early on in the life cycle of a technology, there are many concerns about how these technologies will be used. Some of these are legitimate concerns, while others are based more on misunderstandings about the technology (for example, the quote above that phones could transmit germs). There are also many questions about the right way of deploying these technologies. Businesses have not worked out how to convey the right value propositions to consumers, and society has not worked out what is and is not acceptable use of these technologies. Many of these concerns are lumped together under the rubric of "privacy," or "invasiveness," forming a "privacy hump" that represents a barrier to the acceptance of a potentially intrusive technology.

Over time, however, the concerns may fade, especially if the value proposition of the technology is strong enough. The worst fears do not materialize, society adapts to the technology, and laws are passed to punish violators. An example of the former is that most people understand it is appropriate to take a photo at a wedding but not at a funeral.



Pessimistic Phase

- Reactions:
  - Many legitimate concerns
  - Alarmist reactions
- Main research questions:
  - "Right" way to deploy / facilitate adoption
  - Value proposition
  - Rules of fair use

Optimistic Phase

- Reactions:
  - Users become comfortable with technology
  - Concerns assuaged by positive experience
- Main research questions:
  - How to cement "Architecture of privacy" (Market, Legal, Social, Technical elements)
  - How to optimize application value and minimize risks going forward

Fig. 4.2 The Privacy Hump, a working hypothesis describing the acceptance of potentially intrusive technologies. Early in the life cycle of a technology, users have concerns about how the technology will be used, often couched in terms of privacy. However, if, over time, privacy violations do not occur, and a system of market, social, legal, and technical forces addresses legitimate concerns, then a community of users can overcome the hump and the technology is accepted.

An example of the latter are "do not call" lists that protect individuals from telemarketers and laws punishing camera voyeurs [286].

In other words, if a large enough community of users overcomes the "privacy hump," it is not because their privacy concerns disappear, but because the entire system — the market, social norms, laws, and technology [195] — adapt to make these concerns understandable and manageable. It should be noted, that the privacy hump cannot always be overcome. For example, nurses have rejected the use of locator badges in more than one instance [16, 53].

The "privacy hump" hypothesis is an educated speculation, and it is not clear to us how to acquire empirical evidence to confirm or refute it. However, if this predictive model is correct, it would suggest many directions for future research. For example, research could investigate what factors contribute to the concerns expressed by a community of users. This might include better ways of tailoring new technologies to different categories of people, perhaps along the fundamentalist/pragmatist/unconcerned continuum (as described Section 3.1.1) or along an innovators/early adopters/early majority/late majority/laggards spectrum, as described by Rogers [245].

Other work could investigate what UIs, value propositions, and policies flatten the peak of the privacy hump and accelerate the process of acceptance (assuming a positive judgment by the designer that a given technology ought to be accepted) [154]. For example, we mentioned earlier in Section 4.5.1, when recounting PARC's ubicomp experience, how poor framing of a technology severely impacted its acceptance.

Finally, personal experience may affect an individual's conception of privacy risks. For example, a preliminary study conducted by Pew Internet and American Life suggests that when people first use the Internet, they are less likely to engage in risky activities such as buying online or chatting with strangers, but are more likely to do so after a year of experience [233]. Understanding the privacy hump from these perspectives would be useful, because it would help us to understand how to better design and deploy technologies, how to increase the likelihood of their acceptance, and what acceptance timeline to expect.

5

Conclusions

In the past ten years, privacy has become a mainstream topic in HCI research, as attested by the growing number of surveys, studies, and experiments in this area. In this article, we presented a survey of this rich and diverse landscape, describing some of the legal foundations and historical aspects of privacy, sketching out an overview of the body of knowledge with respect to designing, implementing, and evaluating privacy-affecting systems, and charting many directions for future work.

We believe that the strong interest in and growth of this field is a response to legitimate concerns arising from the introduction of new technologies, and is, overall, a positive development. However, understanding privacy requires HCI practitioners to expand their field of view from traditional HCI domains such as social psychology and cognitive science, to a broader picture which includes economics and law.

In Chapter 4, we listed five challenges facing the field today, that must be tackled to advance the current state of the art in this field:

— The development of better interaction techniques and standard defaults that users can easily understand.

- — The development of stronger analysis techniques and survey tools.
- — The documentation of the effectiveness of design tools, and the creation of a "privacy toolbox."
- — The development of organizational support for managing personal data.
- — The development of a rigorous theory of acceptance dynamics of users, specifically related to privacy.

This review shows that work is well already underway in most of these directions, but is still unorganized and dispersed. Our hope that this article, summarizing 30 years of privacy research in HCI and CSCW, helps to shed light on many of the salient issues and will help practitioners and researchers alike explore these complex issues in a more informed and conscious way.

Acknowledgments

We thank Gregory Abowd, Alessandro Acquisti, Ben Bederson, Lorrie Cranor, Paul Dourish, Gillian Hayes, James Finlay, Heather Richter, Norman Sadeh, Karen Tang, and all the reviewers for their help. We are also indebted with countless colleagues in three continents for stimulating intellectual exchanges.

Support for this work was provided by the NSF Graduate Research Fellowship Program, the President of Georgia Tech, the Dean of the College of Computing of Georgia Tech, and the MacArthur Foundation through the Sam Nunn Security Program. This work is also supported in part by Intel Research, NSF Grants CNS-0627513 ("User-Controllable Security and Privacy for Pervasive Computing") and IIS-0534406 ("Next Generation Instant Messaging: Communication, Coordination, and Privacy for Mobile, Multimodal, and Location-Aware Devices"), and ARO research grant DAAD19-02-1-0389 ("Perpetually Available and Secure Information Systems") to Carnegie Mellon University's CyLab.

Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the agencies above.

References

[1] B. Aalberts and S. van der Hof, *Digital Signature Blindness — Analysis of Legislative Approaches Toward Electronic Authentication*. Technical Paper, 1999.

[2] M. S. Ackerman, "Privacy in pervasive environments: Next generation labeling protocols," *Personal and Ubiquitous Computing*, vol. 8, pp. 430–439, 2004.

[3] M. S. Ackerman, L. Cranor, and J. Reagle, "Privacy in e-commerce: Examining user scenarios and privacy preferences," in *Proceedings of ACM conference on electronic commerce* (*EC'99*), pp. 1–8, Denver, Colorado, November 1999.

[4] M. S. Ackerman and L. F. Cranor, "Privacy critics: Safe-guarding users' personal data," in *Proceedings of Human Factors in Computing Systems: CHI '99*, pp. 258–259, 1999.

[5] M. S. Ackerman and S. D. Mainwaring, "Privacy issues and human-computer interaction," in *Security and Usability: Designing Secure Systems that People Can Use*, (S. Garfinkel and L. Cranor, eds.), pp. 381–400, Sebastopol, CA, USA: O'Reilly, 2005.

[6] M. S. Ackerman, B. Starr, D. Hindus, and S. D. Mainwaring, "Hanging on the wire: A field study of an audio-only media space," *ACM Transactions on Computer-Human Interaction* (*TOCHI*), vol. 4, no. 1, 1997.

[7] A. Acquisti, "Protecting privacy with economics: Economic incentives for preventive technologies in ubiquitous computing environments," in *Proceedings of Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing* (*UBICOMP 02*), Goteborg, Sweden. http://guir.berkeley.edu/privacyworkshop2002/, 2002.

[8] A. Acquisti and J. Großklags, "Privacy and rationality in individual decision making," *IEEE Security and Privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[9] A. Adams, “Multimedia information changes the whole privacy ball game,” in *Proceedings of Computers, Freedom, and Privacy*, pp. 25–32, Toronto, Canada: ACM Press, 2000.

[10] A. Adams and A. Blandford, “Bridging the gap between organizational and user perspectives of security in the clinical domain,” *International Journal of Human-Computer Studies*, vol. 63, pp. 175–202, 2005.

[11] P. E. Agre, “Surveillance and capture: Two models of privacy,” *The Information Society*, vol. 10, pp. 101–127, 1994.

[12] P. E. Agre, “Changing places: Contexts of awareness in computing,” *Human-Computer Interaction*, vol. 16, no. 2–4, pp. 177–192, 2001.

[13] P. E. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape.* Cambridge MA: MIT Press, 1997.

[14] C. Alexander, *The Timeless Way of Building.* New York, NY, USA: Oxford University Press, 1979.

[15] J. P. Allen, “Controversies about privacy and open information in CSCW: A panel report from the CSCW’92 conference,” *SIGOIS Bull*, vol. 14, no. 1, pp. 19–20, 1993.

[16] allnurses.com, New Restroom protocol per management 2002, http://allnurses.com/t16164.html, 1993.

[17] I. Altman, *The Environment and Social Behavior — Privacy, Personal Space, Territory, Crowding.* Monterey, CA: Brooks/Cole Publishing Company, 1975.

[18] E. Ammenwerth, A. Buchauer, H.-B. Bludau, and A. Roßnagel, “Simulation studies for the evaluation of security technology,” in *Multilateral Security in Communications: Technology, Infrastructure, Economy*, (G. Müller and K. Rannenberg, eds.), pp. 547–560, Addison-Wesley Longman Verlag GmbH, 1999.

[19] R. Anderson, “Why cryptosystems fails,” *Communications of the ACM*, vol. 37, no. 11, 1994.

[20] A. Anton, Q. He, and D. Baumer, “The complexity underlying JetBlue’s privacy policy violations,” *IEEE Security and Privacy*, vol. 2, no. 6, pp. 12–18, 2004.

[21] A. I. Anton and J. B. Earp, “A requirements taxonomy for reducing Web site privacy vulnerabilities,” *Requirements Engineering*, vol. 9, pp. 169–185, 2004.

[22] P. M. Aoki and A. Woodruff, “Making space for stories: Ambiguity in the design of personal communication systems,” in *Proceedings of Human Factors in Computing Systems* (*CHI 2005*), pp. 181–190, Portland, OR, USA: ACM Press, 2005.

[23] M. Arnold, “On the phenomenology of technology: The ‘Janus-faces’ of mobile phones,” *Information and Organization* (*Information and Organization*), vol. 13, pp. 231–256, 2003.

[24] P. Ashley, M. Schunter, and C. Powers, “From privacy promises to privacy management — A new approach for enforcing privacy throughout an enterprise,” in *Proceedings of New Security Paradigms Workshop*, pp. 43–50, Virginia Beach, VA: ACM Press.

[25] Association for Computing Machinery, ACM Code of Ethics. http://www.acm.org/serving/ethics.html.

[26] D. Avrahami, D. Gergle, S. E. Hudson, and S. Kiesler, "Improving the accuracy of cell phone interruptions: A study on the effect of contextual information on the behaviour of callers," *Behavior And Information Technology*, vol. 26, no. 3, pp. 247–259, 2007.

[27] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly*, vol. 30, no. 1, pp. 13–28, 2006.

[28] B. Brunk, Understanding the Privacy Space. http://www.firstmonday.org/issues/issue7_10/brunk/, 2002.

[29] E. Ball, D. W. Chadwick, and D. Mundy, "Patient privacy in electronic prescription transfer," *IEEE Security and Privacy*, vol. 1, no. 2, pp. 77–80, 2003.

[30] L. Barkhuus and A. Dey, "Location-based services for mobile telephony: A study of users' privacy concerns," in *Proceedings of Interact 2003, 9th IFIP TC13 International Conference on Human-Computer Interaction*, pp. 709–712, Zurich, Switzerland: ACM Press, 2003.

[31] D. L. Baumer, J. B. Earp, and P. S. Evers, "Tit for tat in cyberspace: Consumer and website responses to anarchy in the market for personal information," *North Carolina Journal of Law and Technology*, vol. 4, no. 2, pp. 217–274, 2003.

[32] BBC News, "Radio tags spark privacy worries," http://news.bbc.co.uk/1/hi/technology/3224920.stm, 2003.

[33] R. Beckwith, "Designing for ubiquity: The perception of privacy," *IEEE Pervasive*, vol. 2, no. 2, pp. 40–46, 2002.

[34] J. Begole, J. C. Tang, R. B. Smith, and N. Yankelovich, "Work rhythms: Analyzing visualizations of awareness histories of distributed groups," in *Proceedings of CSCW'02*, pp. 16–20, New Orleans, LA, USA: ACM Press, November 2002.

[35] J. B. Begole, N. E. Matsakis, and J. C. Tang, "Lilsys: Sensing unavailability," in *Proceedings of Conference on Computer Supported Cooperative Work*, Chicago: ACM Press, 2004.

[36] E. Bekkering and J. P. Shim, "Trust in videoconferencing," *Communications of the ACM*, vol. 49, no. 7, pp. 103–107, 2006.

[37] V. Bellotti, "Design for privacy in multimedia computing and communications environments," in *Technology and Privacy: The New Landscape*, (P. Agre and M. Rotenberg, eds.), Cambridge, MA, USA: MIT Press, 1997.

[38] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," in *Proceedings of The Third European Conference on Computer Supported Cooperative Work (ECSCW'93)*, Milan, Italy: Kluwer Academic Publishers, 1993.

[39] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in e-commerce: Stated preferences vs. actual behavior," *Communications of the ACM*, vol. 48, no. 4, pp. 101–106, 2005.

[40] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[41] J. Berleur and K. Brunnstein, *Ethics of Computing: Codes, Spaces for Discussion and Law.* London, England: Chapman & Hall, 1996.

[42] M. Blackburn, “HIPAA, heal thyself,” *Johns Hopkins Magazine*, vol. 56, no. 5, 2004.

[43] D. Boyd, *Faceted Id/Entity: Managing Representation in a Digital World,* Unpublished Master’s Thesis. Cambridge, MA: MIT, 2002.

[44] M. Boyle, C. Edwards, and S. Greenberg, “The effects of filtered video on awareness and privacy,” in *Proceedings of ACM CSCW 2000*, pp. 1–10, ACM Press, 2000.

[45] M. Boyle and S. Greenberg, “The language of privacy: Learning from video media space analysis and design,” *ACM Transactions on Computer-Human Interaction* (*TOCHI*), vol. 12, no. 2, 2005.

[46] D. Brin, *The Transparent Society.* Reading, MA: Perseus Books, 1998.

[47] British institute of international and comparative law, *The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data.* Technical Report, 2003.

[48] S. Brostoff and M. A. Sasse, “Safe and sound: A safety-critical design approach to security,” in *Proceedings of New Security Paradigms Workshop 2001*, pp. 41–50, Cloudcroft, NM: ACM Press, September 2001.

[49] P. Brusilovsky, A. Kobsa, and W. Nejdl, *The Adaptive Web: Methods and Strategies of Web Personalization.* Heidelberg, Germany: Springer Verlag, 2007.

[50] M. Buchenau and J. F. Suri, “Experience prototyping,” in *Proceedings of DIS 2000: Designing Interactive Systems*, pp. 424–433, ACM Press, 2000.

[51] S. Byers, L. F. Cranor, D. Kormann, and P. McDaniel, “Searching for privacy: Design and implementation of a P3P-enabled search engine,” in *Proceedings of Workshop on Privacy Enhancing Technologies* (*PET2004*), 2004.

[52] J. Cadiz and A. Gupta, *Privacy Interfaces for Collaboration.* Technical Report MSR-TR-2001-82, Redmond, WA: Microsoft Research, 2001.

[53] California Nurses Association, *Eden RNs Protest Electronic Tracking Devices: Mass Turn-in of Nurse Locator Buttons.* http://www.calnurse.org/cna/press/90402a.html, 2002.

[54] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *Communications of the ACM* (*Communications of the ACM*), vol. 24, no. 2, pp. 84–88, 1981.

[55] E. Chung, J. Hong, J. Lin, M. Prabaker, J. Landay, and A. Liu, “Development and evaluation of emerging design patterns for ubiquitous computing,” in *Proceedings of DIS 2004: Designing Interactive Systems*, pp. 233–242, Boston, MA, USA: ACM Press, 2004.

[56] C. F. Citro, D. R. Iglen, and C. B. Marrett, eds., *Protecting Participants and Facilitating Social and Behavioral Sciences Research.* Washington, DC, USA: National Academies Press, 2003.

[57] M. Colbert, “A diary study of rendezvousing: Implications for position-aware computing and communications for the general public,” in *Proceedings of 2001 International ACM SIGGROUP Conference on Supporting Group Work*, pp. 15–23, Boulder, Colorado, USA: ACM Press. http://doi.acm.org/10.1145/500286.500292, 2001.

[58] Commission of the European Communities, *First report on the implementation of the Data Protection Directive (95/46/EC)*. Technical Report COM(2003) 265 final, Commission of the European Communities, Brussels, Belgium, 2003.

[59] S. Consolvo, I. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations: Why, when, and what people want to share," in *Proceedings of CHI 2005, Conference on Human Factors in Computing Systems*, pp. 82–90, ACM Press, 2005.

[60] C. Cool, R. S. Fish, R. Kraut, and C. M. Lowery, "Iterative design of video communication systems," in *Proceedings of CSCW 92*, pp. 25–32, ACM Press, November 1992.

[61] Council of Europe, *The European Convention on Human Rights*. Technical Report, Rome, Italy, 1950.

[62] P. Coy, "Big brother, pinned to your chest," *Business Week*, vol. 3279, August 17, 1992.

[63] L. Cranor, "'I didn't buy it for myself': Privacy and ecommerce personalization," in *Proceedings of Workshop on Privacy in the Electronic Society*, Washington, DC, USA: ACM Press, 2003.

[64] L. Cranor, "What do they 'Indicate?': Evaluating security and privacy indicators," *Interactions*, vol. 13, no. 3, pp. 45–57, 2006.

[65] L. Cranor, P. Guduru, and M. Arjula, "User interfaces for privacy agents," *ACM Transactions on Computer-Human Interaction*, vol. 13, no. 2, pp. 135–178, 2006.

[66] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, The Platform for Privacy Preferences 1.0 (P3P1.0) specification. W3C. http://www.w3.org/TR/P3P/, 2000.

[67] L. F. Cranor and S. Garfinkel, *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA, USA: O'Reilly, 2005.

[68] L. F. Cranor, J. I. Hong, and M. Reiter, *Usable Privacy and Security: Course Overview Lecture Notes*. http://cups.cs.cmu.edu/courses/ups-sp06/slides/060117-overview.ppt, 2006.

[69] L. F. Cranor, M. Langheinrich, and M. Marchiori, "A P3P preference exchange language 1.0 (APPEL1.0)," World Wide Web Consortium Working Draft. http://www.w3.org/TR/WD-P3P-Preferences, 2002.

[70] L. F. Cranor, J. Reagle, and M. S. Ackerman, "Beyond concern: Understanding net users' attitudes about online privacy," in *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*, (I. Vogelsang and B. M. Compaine, eds.), pp. 47–70, Cambridge, MA: MIT Press, 2000.

[71] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science*, vol. 10, no. 1, pp. 104–115, 1999.

[72] M. R. Curry, D. J. Phillips, and P. M. Regan, "Emergency response systems and the creeping legibility of people and places," *The Information Society*, vol. 20, no. 5, pp. 357–369, 2004.

[73] C. Darrah, J. English-Lueck, and J. Freeman, *Familes and Work: An Ethnography of Dual Career Families*. http://www2.sjsu.edu/depts/anthropology/svcp/SVCPslnr.html, 2001.

[74] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, 1989.

[75] S. Davis and C. Gutwin, "Using relationship to control disclosure in Awareness servers," in *Proceedings of 2005 Conference on Graphics interface*, pp. 145–152, Canadian Human-Computer Communications Society, School of Computer Science, University of Waterloo, Waterloo, Ontario, 2005.

[76] Department of Health and Human Services National Institutes of Health, and Office For Protection from Research Risks, Protection of Human Subjects, 2001.

[77] B. M. DePaulo and D. A. Kashy, "Everyday lies in close and casual relationships," *Journal of Personality and Social Psychology*, vol. 74, no. 1, pp. 63–79, 1998.

[78] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), in *Official Journal of the European Communities*, L281, pp. 37–47, 2002.

[79] 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, in *Official Journal of the European Communities*, pp. 31–50, 1995.

[80] S. Doheny-Farina, "The last link: Default = Offline, or why ubicomp scares me," *Computer-mediated Communication*, vol. 1, no. 6, pp. 18–20, 1994.

[81] P. Dourish and K. Anderson, *Privacy, Security ... and Risk and Danger and Secrecy and Trust and Morality and Identity and Power: Understanding Collective Information Practices.* Technical Report UCI-ISR-05-1, Institute for Software Research, University of California at Irvine, Irvine, CA, USA, 2005.

[82] P. Dourish, B. E. Grinter, J. D. D. L. Flor, and M. Joseph, "Security in the wild: User strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, 2004.

[83] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proceedings of Pervasive 2005*, pp. 152–170, Munich, Germany: Springer Verlag, 2005.

[84] E. S. Dunn, "The idea of a national data center and the issue of personal privacy," *The American Statistician*, vol. 21, no. 1, pp. 21–27, 1967.

[85] M. R. Ebling, B. E. John, and M. Satyanarayanan, "The importance of translucence in mobile computing systems," *ACM Transactions on Computer-Human Interaction* (*TOCHI*), vol. 9, no. 1, pp. 42–67, 2002.

[86] S. Egelman, L. F. Cranor, and A. Chowdhury, "An analysis of P3P-enabled web sites among top-20 search results," in *Proceedings of Eighth International Conference on Electronic Commerce*, pp. 14–16, Fredericton, New Brunswick, Canada, August 2006.

[87] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti, "Studying the impact of privacy information on online purchase decisions," in *Proceedings of 2006 CHI Privacy Methods Workshop*, Montreal, Quebec, Canada, 2006.

[88] P. Ehn and M. Kyng, "The collective approach to systems design," in *Computers and Democracy: A Scandinavian Challenge*, (G. Bjerkes, P. Ehn, and M. Kyng, eds.), pp. 17–58, Aldershot, Great Britain: Avebury, 1987.

[89] Electronic Privacy Information Center (EPIC) and Junkbusters, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy.* http://www.epic.org/reports/prettypoorprivacy.html, 2000.

[90] T. Erickson and W. A. Kellogg, "Social translucence: An approach to designing systems that support social processes," *ACM Transactions on Computer-Human Interaction* (*TOCHI*), vol. 7, no. 1, pp. 59–83, 2000.

[91] J. Espey, G. Rudinger, and H. Neuf, "Excessive demands on users of technology," in *Multilateral Security in Communications: Technology, Infrastructure, Economy*, (G. Müller and K. Rannenberg, eds.), pp. 439–449, Addison-Wesley Longman Verlag GmbH, 1999.

[92] B. Esslinger and D. Fox, "Public key infrastructures in banks — Enterprise-wide PKIs," in *Multilateral Security in Communications: Technology, Infrastructure, Economy*, (G. Müller and K. Rannenberg, eds.), pp. 283–300, Addison-Wesley Longman Verlag GmbH, 1999.

[93] A. Etzioni, *The Limits of Privacy.* New York: Basic Books, 1999.

[94] European Commission, *Information Technology Security Evaluation Criteria.* Technical Report, Version 1.2, June 1991.

[95] European Commission Article 29 Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.* Technical Report 11750/02/EN WP 89, 2004.

[96] European Commission Article 29 Working Party, *Opinion on More Harmonised Information Provisions.* Technical Report 11987/04/EN WP 100, European Commission, November 25 2004.

[97] European Commission Article 29 Working Party, *Working Document on Biometrics.* Technical Report 12168/02/EN WP80, 2004.

[98] European Opinion Research Group EEIG, *Special Eurobarometer Data Protection Executive Summary.* Technical Report Special Eurobarometer 196 — Wave 60.0, European Commission, Bruxelles, Belgium, December 2003.

[99] D. Fallman, "Design-oriented human-computer interaction," in *Proceedings of CHI 2003*, pp. 225–232, Ft. Lauderdale, Florida, USA: ACM Press, April 5–10 2003.

[100] Federal Trade Commission, *In the Matter of CardSystems Solutions, Inc., and Solidus Networks, Inc., Doing Business as Pay By Touch Solutions — Complaint.* Technical Report File No. 052 3148, Federal Trade Commission, February 23 2006.

[101] J. Feng, "A brief review of research methods in privacy studies," in *Proceedings of Privacy Methods Workshop at CHI 2006*, Montreal, Quebec, Canada, 2006.

[102] C. S. Fischer, *America Calling: A Social History of the Telephone to 1940.* University of California Press, p. 424, 1994.

[103] G. Fischer, A. C. Lemke, T. Mastaglio, and A. I. Morch, "Using critics to empower users," in *Proceedings of Conference on Human Factors in Computing Systems*, pp. 337–347, Seattle, WA, USA: ACM Press, New York, NY. http://doi.acm.org/10.1145/97243.97305, 1990.

[104] R. Fish, R. E. Kraut, R. W. Root, and R. E. Rice, "Evaluating video as a technology for informal communication," in *Proceedings of Human Factors in Computing Systems* (*CHI 92*). http://doi.acm.org/10.1145/142750.142755, 1992.

[105] J. Fogarty, J. Lai, and J. Christensen, "Presence versus availability: The design and evaluation of a context-aware communication client," *International Journal of Human-Computer Studies*, vol. 61, no. 3, pp. 299–317, 2004.

[106] B. J. Fogg and H. Tseng, "The elements of computer credibility," in *Proceedings of SIGCHI Conference on Human Factors in Computing Systems: CHI 1999*, pp. 80–87, Pittsburgh, PA, USA: ACM Press, http://doi.acm.org/10.1145/302979.303001, May 15–20 1999.

[107] G. Foresti, P. Mähönen, and C. Regazzoni, eds., *Multimedia video-based surveillance systems: Requirements, Issues and Solutions*. Norwell, MA, USA: Kluwer Academic Publishers, 2000.

[108] B. Friedman, "Value-sensitive design," *Interactions: New Visions of Human-Computer Interaction*, vol. 3, no. 6, pp. 17–23, 1996.

[109] B. Friedman, D. C. Howe, and E. Felten, "Informed consent in the mozilla browser: Implementing value-sensitive design," in *Proceedings of The Thirty-Fifth Annual Hawai'i International Conference on System Sciences*, *IEEE Computer Society*, 2002.

[110] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum, "Users' conceptions of web security: A comparative study," in *Proceedings of CHI '02 Extended Abstracts on Human Factors in Computing Systems*, pp. 764–747, Minneapolis, MN, USA, April 20–25 2002.

[111] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*. p. 395, Addison-Wesley, 1995.

[112] S. Garfinkel, "Adopting fair information practices to low cost RFID systems," in *Proceedings of Ubiquitous Computing 2002 Privacy Workshop*. http://www.teco.edu/∼philip/ubicomp2002ws/, 2002.

[113] W. Gaver, J. Beaver, and S. Benford, "Ambiguity as a resource for design," in *Proceedings of CHI 2003*, pp. 233–240, Ft. Lauderdale, FL, USA: ACM Press, 2003.

[114] W. Gaver, T. Moran, A. MacLean, L. Lovstrand, P. Dourish, K. Carter, and W. Buxton, "Realizing a video environment: EuroPARC's RAVE system," in *Proceedings of CHI'92*, pp. 27–35, Monterey, CA, USA: ACM Press, May 1992.

[115] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: Adoption criteria in encrypted email," in *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*, pp. 591–600, Montréal, Québec, Canada: ACM Press, http://doi.acm.org/10.1145/1124772.1124862, April 22–27 2006.

[116] German Constitutional Court Volkszählungsurteil vom 15 BVerfGE 65, (Bundesverfassungsgerichts), http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm, 1983.

[117] A. Giddens, *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford, CA, USA: Stanford University Press, 1991.

[118] J. Gideon, S. Egelman, L. F. Cranor, and A. Acquisti, "Power strips, prophylactics, and privacy, oh my!," in *Proceedings of The 2006 Symposium on Usable Privacy and Security (SOUPS 2006)*, pp. 133–144, Pittsburgh, PA, 2006.

[119] E. Goffman, *The Presentation of Self in Everyday Life.* New York: Anchor, Doubleday, 1959.

[120] E. Goffman, *Behavior In Public Places.* Free Press, 1966.

[121] I. Goldberg, "Privacy-enhancing technologies for the Internet, II: Five years later," in *Proceedings of Privacy Enhancing Technologies 2002*, pp. 99–109, LNCS 2482, Springer Verlag, 2002.

[122] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Onion routing for anonymous and private internet connection," *Communication of ACM*, vol. 42, no. 2, pp. 39–41, 1999.

[123] N. S. Good, R. Dhamija, J. Grossklags, D. Thaw, S. Aronowitz, D. Mulligan, and J. Konstan, "Stopping spyware at the gate: A user study of privacy, notice and spyware," in *Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2005*, pp. 43–52, Pittsburgh, PA, USA: ACM Press, July 6–8 2005.

[124] N. S. Good and A. Krekelberg, "Usability and privacy: A study of KaZaA P2P file-sharing," in *Proceedings of CHI 2003*, pp. 137–144, ACM Press. http://portal.acm.org/citation.cfm?id=1073001.1073006, 2003.

[125] A. Grasso and J.-L. Meunier, "Who can claim complete abstinence from peeking at print jobs?," in *Proceedings of CSCW '02*, pp. 296–305, ACM Press, 2002.

[126] W. D. Gray, B. E. John, and M. E. Atwood, "Project ernestine: Validating a GOMS analysis for predicting and explaining real-world performance," *Human-Computer Interaction*, vol. 8, no. 3, pp. 237–309, 1993.

[127] R. E. Grinter and L. Palen, "Instant messaging in teenage life," in *Proceedings of ACM Conference on Computer Supported Cooperative Work (CSCW2002)*, pp. 21–30, ACM Press. http://doi.acm.org/10.1145/587078.587082, 2004.

[128] R. Gross and A. Acquisti, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Proceedings of Privacy Enhancing Technologies*, p. 18, 2006.

[129] J. Grudin, "Groupware and social dynamics: Eight challenges for developers," *Communications of the ACM*, vol. 37, no. 1, pp. 92–105, 1994.

[130] J. Grudin, "Desituating action: Digital representation of context," *Human-Computer Interaction (HCI) Journal*, vol. 16, no. 2–4, 2001.

[131] J. Grudin, "Three faces of human-computer interaction," *Annals of the History of Computing*, vol. 27, no. 4, pp. 46–62, 2005.

[132] J. Grudin and E. Horvitz, "Presenting choices in context: Approaches to information sharing," Workshop on Ubicomp communities: Privacy as Boundary Negotiation, http://guir.berkeley.edu/pubs/ubicomp2003/privacyworkshop/papers.htm, 2003.

[133] M. Gruteser and D. Grunwald, "A methodological assessment of location privacy risks in wireless hotspot networks," in *Proceedings of Security in Pervasive Computing Conference*, pp. 10–24, Boppard, Germany: Springer Verlag, 2004.

[134] GVU Center, *10th WWW User Survey — Online Privacy and Security.* Technical Report, GVU Center, Georgia Insitute of Technology, 1999. http://guv.cc.gatech.edu.

[135] J. Häkkilä and C. Chatfield, "Toward social mobility: 'It's like if you opened someone else's letter': User perceived privacy and social practices with SMS communication," in *Proceedings of Human Computer Interaction with Mobile Devices and Services MobileHCI '05*, pp. 219–222, Salzburg, Austria: ACM Press, http://doi.acm.org/10.1145/1085777.1085814, September 2005.

[136] J. T. Hancock, J. Thom-Santelli, and T. Ritchie, "Deception and design: The impact of communication technology on lying behavior," in *Proceedings of CHI 2004*, pp. 129–134, Vienna, Austria: ACM Press, 24–29 April 2004.

[137] R. H. Harper, "Why people do and don't wear active badges: A case study," in *Proceedings of Computer Supported Cooperative Work* (*CSCW96*), pp. 297–318, ACM Press, 1996.

[138] Harris Interactive, *IBM Multi-National Consumer Privacy Survey.* Technical Report, 1999.

[139] K. Hawkey and K. M. Inkpen, "Keeping up appearances: Understanding the dimensions of incidental information privacy," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 821–830, Montréal, Québec, Canada: ACM Press, 2006.

[140] G. R. Hayes and G. Abowd, "Tensions in designing capture technologies for an evidence-based care community," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 937–946, Montréal, Québec, Canada: ACM Press, 2006.

[141] L. M. Hilty, C. Som, and A. Köhler, "Assessing the human, social and environmental risks of pervasive computing," *Human and Ecological Risk Assessment*, vol. 10, pp. 853–874, 2004.

[142] D. Hindus, M. Ackerman, S. D. Mainwaring, and B. Starr, "Thunderwire: A field study of an audio-only media space," in *Proceedings of Computer Supported Cooperative Work '96*, pp. 238–247, Cambridge, MA, USA: ACM Press, 1996.

[143] D. Hindus, S. D. Mainwaring, N. Leduc, A. E. Hagström, and O. Bayley, "Casablanca: Designing social communication devices for the home," *CHI Letters* (*Human Factors in Computing Systems: CHI 2001*), vol. 3, no. 1, pp. 325–332, 2001.

[144] H. Hochheiser, "The platform for privacy preference as a social protocol: An examination within the US policy context," *ACM Transactions on Internet Technology*, vol. 2, no. 4, pp. 276–306, 2002.

[145] K. Holtzblatt and H. Beyer, *Contextual Design: A Customer-Centered Approach to Systems Designs.* Morgan-Kaufmann, 1997.

[146] J. Hong, J. D. Ng, S. Lederer, and J. A. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," in *Proceedings of Designing Interactive Systems* (*DIS2004*), pp. 91–100, Boston, MA: ACM Press, 2004.

[147] J. M. Hudson and A. Bruckman, "Using empirical data to reason about internet research ethics," in *Proceedings of ECSCW '05*, pp. 287–306, Paris, France: Springer Verlag, 18–22, September 2005.

[148] S. Hudson and I. Smith, "Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems," in *Proceedings of CSCW '96*, pp. 248–257, ACM Press. http://doi.acm.org/10.1145/240080.240295, 1996.

[149] B. Husted, "ChoicePoint's fine sets record," *Atlanta Journal-Constitution*, Jan 27 2006.

[150] G. Iachello, "Protecting personal data: Can IT security management standards help?," in *Proceedings of ACSAC 2003*, pp. 266–275, Las Vegas, Nevada, USA: IEEE Press, December 2003.

[151] G. Iachello, *Privacy and Proportionality*. Unpublished Doctoral Dissertation, Georgia Inst. of Technology, Atlanta, GA, USA, http://etd.gatech.edu, 2006.

[152] G. Iachello and G. D. Abowd, "Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing," in *Proceedings of CHI 2005*, pp. 91–100, Portland, OR, USA: ACM Press, 2005.

[153] G. Iachello, I. Smith, S. Consolvo, M. Chen, and G. D. Abowd, "Developing privacy guidelines for social location disclosure applications and services," in *Proceedings of Symposium on Usable Privacy and Security* (*SOUPS*), pp. 65–76, Pittsburgh, PA, USA: ACM Press, July 6–8 2005.

[154] G. Iachello, K. N. Truong, G. D. Abowd, G. R. Hayes, and M. Stevens, "Experience prototyping and sampling to evaluate ubicomp privacy in the real world," in *Proceedings of CHI 2006*, pp. 1009–1018, Montreal, Canada: ACM Press, 2006.

[155] IBM Corporation, *Privacy is good for business*. http://www.ibm.com/innovation/us/customerloyalty/harriet_pearson_interview.shtml, 2007.

[156] International Labor Organization, "*Workers Privacy Part II: Monitoring and Surveillance in the Workplace Conditions of Work*," Special Series on Workers Privacy, Digest 12, no. 1, 1993.

[157] International Organization for Standardization/International Electrotechnical Commission, *IS17799:2000 Information Technology — Code of Practice for Information Security Management*. 2000.

[158] M. Ito and O. Daisuke, "Mobile phones, Japanese youth and the replacement of social contact," in *Front Stage/Back Stage: Mobile Communication and the Renegotiation of the Social Sphere*, (R. Ling and P. Pedersen, eds.), pp. 65–76, Grimstad, Norway, 2003.

[159] A. R. Jacobs and G. D. Abowd, "A framework for comparing perspectives on privacy and pervasive technologies," *IEEE Pervasive Computing*, vol. 2, no. 4, pp. 78–84, 2003.

[160] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *To appear in Communication of ACM*, 2007.

[161] G. Jancke, G. D. Venolia, J. Grudin, J. Cadiz, and A. Gupta, "Linking public spaces: Technical and social issues," *CHI Letters* (*Human Factors in Computing Systems: CHI 2001*), vol. 3, no. 1, pp. 530–537, 2001.

[162] U. Jendricke and D. Gerd tom Markotten, "Usability meets security: The identity-manager as your personal security assistant for the internet," in *16th Annual Computer Security Applications Conference* (*ACSAC 00*), New Orleans, LA, USA, 2000.

[163] C. Jensen, *Designing For Privacy in Interactive Systems.* Unpublished Doctoral Dissertation, Georgia Institute of Technology, Atlanta, GA, USA, http://etd.gatech.edu, 2005.

[164] C. Jensen and C. Potts, "Privacy policies as decision-making tools: An evaluation of online privacy notices," in *Proceedings of CHI 2004*, ACM Press, 2004.

[165] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of Internet users: Self-reports versus observed behavior," *International Journal of Human-Computer Studies*, vol. 63, pp. 203–227, 2005.

[166] C. Jensen, J. Tullio, C. Potts, and E. D. Mynatt, *STRAP: A Structured Analysis Framework for Privacy.* Technical Report GVU Technical Report 05-02, GVU Center, Georgia Institute of Technology, Atlanta, GA, USA, January 2005.

[167] A. Jesdanun, "AOL: Breach of privacy was a mistake," *Associated Press Financial Wire*, 2006.

[168] X. Jiang, J. I. Hong, and J. A. Landay, "Approximate information flows: Socially-based modeling of privacy in ubiquitous computing," in *Proceedings of Ubicomp 2002*, pp. 176–193, Göteborg, Sweden: Springer Verlag, 2002.

[169] S. Junestrand, U. Keijer, and K. Tollmar, "Private and public digital domestic spaces," *International Journal of Human-Computer Studies*, vol. 54, no. 5, pp. 753–778, 2001.

[170] E. Kaasinen, "User needs for location-aware mobile services," *Personal and Ubiquitous Computing*, vol. 7, no. 1, pp. 70–79, 2003.

[171] S. Karas, "Privacy, identity, databases," *American University Law Review*, vol. 52, p. 393, 2003.

[172] C.-M. Karat, J. Karat, C. Brodie, and J. Feng, "Evaluating interfaces for privacy policy rule authoring," in *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*, pp. 83–92, Montréal, Québec, Canada: ACM Press, April 22–27 2006. http://doi.acm.org/10.1145/1124772.1124787.

[173] A. M. Keller, D. Mertz, J. Hall, and A. Urken, "Privacy issues in an electronic voting machine," in *Proceedings of 2004 ACM workshop on Privacy in the electronic society*, pp. 33–34, ACM Press, October 2004.

[174] T. Kindberg, A. Sellen, and E. Geelhoed, "Security and trust in mobile interactions: A study of users' perceptions and reasoning," in *Proceedings of Ubicomp 2004*, pp. 196–213, Nottingham, UK: Springer Verlag, September 7–10 2004.

[175] S. Kinzie and Y. Noguchi, "In online social club, sharing is the point until it goes too far," *Washington Post*, p. A01, 2006.

[176] R. Kling, "Fair information practices with computer supported cooperative work (CSCW)," *Computer-Mediated Communication Magazine*, vol. 1, no. 2, p. 5, 1994.

[177] A. Klinke and O. Renn, "A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies," *Risk Analysis*, vol. 22, no. 6, pp. 1071–1094, 2002.

[178] K. J. Knapp, T. E. Marshall, R. K. Rainer, and D. W. Morrow, *Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)^2 Survey Results.* Technical Report, Auburn University, Auburn, AL, 2004.

[179] A. Kobsa, "Personalized hypermedia and international privacy," *Communications of the ACM*, vol. 45, no. 5, pp. 64–67, 2002.

[180] A. Kobsa and J. Schreck, "Privacy through pseudonymity in user-adaptive systems," *ACM Transactions on Internet Technology* (*TOIT*), vol. 3, no. 2, 2003.

[181] J. Kontio, L. Lehtola, and J. Bragge, "Using the focus group method in software engineering: Obtaining practitioner and user experiences," in *Proceedings of International Symposium on Empirical Software Engineering* (*ISESE*), pp. 271–280, Redondo Beach, USA: IEEE Computer Society, August 19–20 2004.

[182] B. Kowitz and L. Cranor, "Peripheral privacy notifications for wireless networks," in *Proceedings of Workshop on Privacy In The Electronic Society '05*, pp. 90–96, Alexandria, VA, USA, 2005.

[183] R. E. Kraut, C. Cool, R. E. Rice, and R. S. Fish, "Life and death of new technology: Task, utility and social influences on the use of a communication medium," in *Proceedings of CSCW 94*, pp. 13–21, Chapel Hill, NC, USA: ACM Press, 1994.

[184] P. Kumaraguru and L. F. Cranor, *Privacy Indexes: A Survey of Westin's Studies.* Technical Report CMU-ISRI-05-138, Institute for Software Research International, School of Computer Science, Carnegie Mellon University, December 2005.

[185] S. Lahlou, "Living in a goldfish bowl: Lessons learned about privacy issues in a privacy-challenged environment," in *Proceedings of Privacy Workshop at Ubicomp 2005*, Tokyo Japan, 2005.

[186] M. Langheinrich, "Privacy by design — Principles of privacy-aware ubiquitous systems," in *Proceedings of Ubicomp 2001*, pp. 273–291, Springer Verlag, 2001.

[187] M. Langheinrich, "A privacy awareness system for ubiquitous computing environments," in *Proceedings of Ubicomp 2002*, pp. 237–245, Goteberg, Sweden, 2002.

[188] G. Lasprogata, N. J. King, and S. Pillay, "Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada," *Stanford Technology Law Review*, vol. 4, 2004.

[189] B. Latour, *We've Never Been Modern.* Cambridge, MA, USA: Harvard University Press, 1991.

[190] T. Lau, O. Etzioni, and D. S. Weld, "Privacy interfaces for information management," *Communications of the ACM*, vol. 42, no. 10, pp. 88–94, 1999.

[191] S. Lederer, *Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing.* Unpublished Master of Science, University of California, Berkeley, Berkeley, CA. http://www.cs.berkeley.edu/projects/io/publications/privacy-lederer-msreport-1.01-no-appendicies.pdf, 2003.

[192] S. Lederer, J. I. Hong, A. Dey, and J. A. Landay, "Five pitfalls in the design for privacy," in *Security and Usability*, (S. Garfinkel and L. F. Cranor, eds.), pp. 421–445, 2005.

[193] S. Lederer, J. Mankoff, and A. Dey, "Towards a deconstruction of the privacy space," in *Proceedings of Workshop on Privacy In Ubicomp 2003:*

Ubicomp communities: Privacy as Boundary Negotiation, Seattle, WA, USA. http://guir.berkeley.edu/pubs/ubicomp2003/privacyworkshop/papers/lederer-privacyspace.pdf, 2003.

[194] S. Lederer, J. Mankoff, and A. K. Dey, "Who wants to know what when? Privacy preference determinants in ubiquitous computing," in *Extended Abstracts of CHI 2003, ACM Conference on Human Factors in Computing Systems*, pp. 724–725, Fort Lauderdale, FL, 2003.

[195] L. Lessig, "The architecture of privacy," *Vanderbilt Journal of Entertainment Law and Practice*, vol. 1, p. 56, 1999.

[196] L. Lessig, *Code and Other Laws of Cyberspace*. New York, NY: Basic Books, 1999.

[197] R. Ling, *The Mobile Connection: The Cell Phone's Impact on Society*. Morgan Kaufmann, Third ed., 2004.

[198] W. E. Mackay, "Ethics, lies and videotape . . . ," in *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*, pp. 138–145, ACM Press, 1995.

[199] A. MacLean, R. M. Young, V. Bellotti, and T. P. Moran, "Questions, options, and criteria: Elements of design space analysis," *Human-Computer Interaction* (*HCI*) *Journal*, vol. 6, no. 3&4, pp. 201–250, 1991.

[200] A. MacLean, R. M. Young, and T. P. Moran, "Design rationale: The argument behind the artifact," in *Proceedings of CHI 1989*, pp. 247–252, ACM Press, 1989.

[201] M. M. Maheu, P. Whitten, and A. Allen, eds., *E-Health, Telehealth, and Telemedicine: A Guide to Start-up and Success*. Jossey Bass Health Series: San Francisco, 2001.

[202] W. March and C. Fleuriot, "Girls, technology and privacy: "Is my mother listening?"," in *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*, pp. 107–110, Montréal, Québec, Canada: ACM Press, http://doi.acm.org/10.1145/1124772.1124790, April 22–27 2006.

[203] D. McCullagh, Intel Nixes Chip-Tracking ID. http://www.wired.com/news/politics/0,1283,35950,00.html, 2000.

[204] A. S. Melenhorst, A. D. Fisk, E. D. Mynatt, and W. A. Rogers, "Potential intrusiveness of aware home technology: Perceptions of older adults," pp. 266–270, 2004.

[205] Microsoft Corporation, Protecting Americans' Privacy, http://www.microsoft.com/issues/essays/2007/03-20ProtectingPrivacy.mspx, Issued March 20, 2007.

[206] A. E. Milewski and T. M. Smith, "Providing presence cues to telephone users," in *Proceedings of The 2000 ACM Conference on Computer Supported Cooperative Work* (*CSCW2000*), pp. 89–96, ACM Press, 2000.

[207] L. I. Millett, B. Friedman, and E. Felten, "Cookies and web browser design: Toward realizing informed consent online," *CHI Letters*, vol. 3, no. 1, pp. 46–52, 2001.

[208] K. Mitnick and W. Simon, *The Art of Deception: Controlling the Human Element of Security*. Wiley, First ed., 2002.

[209] J. H. Moor, "Towards a theory of privacy in the information age," *Computers and Society*, vol. 27, no. 3, pp. 27–32, 1997.

[210] G. Müller and K. Rannenberg, eds., *Multilateral Security in Communications Volume 3: Technology, Infrastructure, Economy.* München: Addison-Wesley, 1999.

[211] M. J. Muller, J. G. Smith, J. Z. Shoher, and H. Goldberg, "Privacy, anonymity and interpersonal competition issues identified during participatory design of project management groupware," *ACM SIGCHI Bulletin*, vol. 23, no. 1, 1990.

[212] R. S. Murphy, "Property rights in personal information: An economic defense of privacy," *Georgetown Law Journal*, vol. 84, p. 2381, 1996.

[213] K. Nagel, *Using Availability Indicators to Enhance Context-Aware Family Communication Applications.* Unpublished PhD, Georgia Institute of Technology, Atlanta, GA, USA, 2006.

[214] K. Nagel, J. Hudson, and G. D. Abowd, "Predictors of availability in home life context-mediated communication," in *Proceedings of CSCW'04*, pp. 497–506, ACM Press, 2004. http://etd.gatech.edu.

[215] K. Nagel, C. D. Kidd, T. O'Connell, A. Dey, and G. D. Abowd, "The family intercom: Developing a context-aware audio communication system," in *Proceedings of Ubicomp 2001*, pp. 176–183, Atlanta, GA, 2001.

[216] B. Nardi, S. Whittaker, and E. Bradner, "Interaction and outeraction: Instant messaging in action," in *Proceedings of ACM Conference on Computer Supported Cooperative Work* (*CSCW2000*), pp. 79–88, ACM Press, 2000.

[217] A. Neal, M. Humphreys, D. Leadbetter, and P. Lindsay, "Development of hazard analysis techniques for human-computer systems," in *Innovation and Consolidation in Aviation*, (G. Edkins and P. Pfister, eds.), pp. 255–262, Aldershot, UK: Ashgate, 2003.

[218] C. Neustaedter and S. Greenberg, "The design of a context-aware home media space for balancing privacy and awareness," in *Proceedings of UbiComp 2003*, pp. 297–314, Springer-Verlag, 2003.

[219] C. Neustaedter, S. Greenberg, and M. Boyle, "Blur filtration fails to preserve privacy for home-based video conferencing," *ACM Transactions on Computer Human Interactions* (*TOCHI*), vol. 13, no. 1, pp. 1–36, 2005.

[220] D. H. Nguyen and E. D. Mynatt, "Privacy mirrors: Making ubicomp visible," in *Proceedings of Human Factors in Computing Systems: CHI 2001* (*Workshop on Building the User Experience in Ubiquitous Computing*), Seattle, WA: ACM Press, 2001.

[221] J. Nielsen and R. L. Mack, eds., *Usability Inspection Methods.* New York, NY, USA: John Wiley & Sons, 1994.

[222] D. A. Norman, *The Design of Everyday Things.* New York, NY: Basic Books, 2002.

[223] C. Norris and G. Armstrong, *The Maximum Surveillance Society: The Rise of CCTV.* Oxford, England: Berg, 1999.

[224] J. S. Olson, J. Grudin, and E. Horvitz, "A study of preferences for sharing and privacy," in *Proceedings of CHI '05 Extended Abstracts on Human Factors in Computing Systems*, April 2005.

[225] Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Technical Report, 1980.

[226] L. Palen, "Social, individual and technological issues for groupware calendar systems," *CHI Letters: Human Factors in Computing Systems, CHI 99*, vol. 2, no. 1, pp. 17–24, 1999.

[227] L. Palen and P. Dourish, "Unpacking 'Privacy' for a networked world," *CHI Letters* (*Human Factors in Computing Systems: CHI 2003*), vol. 5, no. 1, pp. 129–136, 2003.

[228] S. Patil and A. Kobsa, "Instant messaging and privacy," in *Proceedings of HCI 2004*, pp. 85–88, Leeds, UK, 2004.

[229] A. Patrick, P. Briggs, and S. Marsh, "Designing systems that people will trust," in *Security and Usability*, (L. Cranor and S. Garfinkel, eds.), pp. 75–99, O'Reilly Media, 2005.

[230] A. S. Patrick and S. Kenny, "From privacy legislation to interface design: Implementing information privacy in human-computer interactions," in *Proceedings of PET 2003*, pp. 107–124, Springer Verlag, 2003.

[231] J. S. Pettersson, S. Fischer-Hübner, N. Danielsson, J. Nilsson, M. Bergmann, S. Clauss, T. Kriegelstein, and H. Krasemann, "Making PRIME usable," in *Proceedings of SOUPS '05*, pp. 53–64, Pittsburgh, PA, USA: ACM Press, 2005.

[232] Pew Internet and American Life, Trust and Privacy Online: Why Americans Want to Rewrite the Rules, http://www.pewinternet.org/reports/toc.asp?Report=19, 2000.

[233] Pew Internet and American Life, Testimony of Lee Rainie: Director, Pew Internet and American Life Project. http://www.pewinternet.org/reports/toc.asp?Report=34, 2001.

[234] A. Pfitzmann, "Technologies for multilateral security," in *Multilateral Security in Communications: Technology, Infrastructure, Economy*, (G. Müller and K. Rannenberg, eds.), pp. 85–91, Addison-Wesley Longman Verlag GmbH, 1999.

[235] R. A. Posner, "An economic theory of privacy," *Regulation*, pp. 19–26, 1978.

[236] D. Povey, "Optimistic security: A new access control paradigm," in *Proceedings of 1999 New Security Paradigms Workshop*, pp. 40–45, ACM Press. http://security.dstc.edu.au/ staff/povey/papers/optimistic.pdf, 1999.

[237] B. A. Price, K. Adam, and B. Nuseibeh, "Keeping ubiquitous computing to yourself: A practical model for user control of privacy," *International Journal on Human-Computer Studies*, vol. 63, pp. 228–253, 2005.

[238] Privacy and American Business, "Consumer privacy attitudes: a major shift since 2000 and why," *Privacy and American Business Newsletter*, vol. 10, no. 6, 2003.

[239] Privacy Protection Study Commission, *Personal Privacy in an Information Society.* Technical Report, Government Printing Office, Washington, DC, USA, 1977.

[240] Rambøll Management Denmark, *Economic Evaluation of the Data Protection Directive 95/46/EC Final Report.* Technical Report, May 2005.

[241] K. Rannenberg, "Recent development in information technology security evaluation — The need for evaluation criteria for multilateral security," in *Proceedings of Security and Control of Information Technology in Society — Proceedings of the IFIP TC9/WG 9.6 Working Conference*, pp. 113–128, Onboard

M/S Ilich and ashore at St. Petersburg, Russia: North-Holland, Amsterdam, August 12–17 1993.

[242] K. Rannenberg, "What can IT security certification do for multilateral security?," in *Multilateral Security in Communications: Technology, Infrastructure, Economy*, (G. Müller and K. Rannenberg, eds.), pp. 515–530, Addison-Wesley Longman Verlag GmbH, 1999.

[243] K. Rannenberg, "Multilateral security: A concept and examples for balanced security," in *Proceedings of New Security Paradigms Workshop*, pp. 151–162, Ballycotton, Ireland: ACM Press, 2000.

[244] H. Rheingold, "PARC is back!," *Wired*, vol. 2, no. 2, 1994.

[245] E. Rogers, *Diffusion of Innovations.* Free Press, Fifth ed., 2003.

[246] R. W. Root, "Design of a multi-media vehicle for social browsing," in *Proceedings of The 1988 ACM Conference on Computer-supported Cooperative Work* (*CSCW 88*), pp. 25–38, ACM Press. http://doi.acm.org/10.1145/62266.62269, 1988.

[247] A. Roßnagel, R. Haux, and W. Herzog, eds., *Mobile und sichere Kommunikation im Gesundheitswesen.* Vieweg: Braunschweig, Germany, 1999.

[248] G. Rowan, "Visionaries see invisible computing," *The Globe and Mail*, 1997.

[249] P. Samuelson, "Privacy as intellectual property?," *Stanford Law Review*, vol. 52, p. 1125, 2000.

[250] A. Sasse, "Computer security: Anatomy of a usability disaster, and a plan for recovery," in *Proceedings of 2003 Workshop on Human-Computer Interaction and Security Systems at CHI 2003.* http://www.andrewpatrick.ca/CHI2003/HCISEC/, 2003.

[251] W. Scacchi, "Socio-technical design," in *The Encyclopedia of Human-Computer Interaction*, (W. S. Bainbridge, ed.), Berkshire Publishing Group, 2004.

[252] S. D. Scalet, "The five most shocking things about the choice point debacle," *CSO Magazine*, 2005.

[253] B. N. Schilit, D. M. Hilbert, and J. Trevor, "Context-aware communication," *IEEE Wireless Communications*, vol. 9, no. 5, pp. 46–54, 2002.

[254] C. Schmandt, J. Kim, K. Lee, G. Vallejo, and M. Ackerman, "Mediated voice communication via mobile IP," in *Proceedings of 15th Annual ACM Symposium on User Interface Software and Technology UIST '02*, pp. 141–150, Paris, France, October 27–30, 2002: ACM Press, http://doi.acm.org/10.1145/571985.572005, 2002.

[255] B. Schneier, *Secrets and Lies: Digital Security in a Networked World.* Vol. xv+412, New York, NY, USA: Wiley Computer Publishing, 2000.

[256] B. Schneier, *Beyond Fear.* New York, NY, USA: Springer, 2006.

[257] K. B. Sheehan, "In poor health: An assessment of privacy policies at direct-to-consumer web sites," *Journal of Public Policy and Marketing*, vol. 24, no. 2, 2005.

[258] B. Shneiderman, "Designing trust into online experiences," *Commununication of ACM*, vol. 43, no. 12, pp. 57–59, 2000.

[259] G. B. Shoemaker and K. M. Inkpen, "Single display privacyware: Augmenting public displays with private information," in *Proceedings of SIGCHI Confer-*

ence on Human Factors in Computing Systems, pp. 522–529, Seattle, WA, USA: ACM Press. http://doi.acm.org/10.1145/365024.365349, 2001.

[260] M. SiteAdvisor, *McAfee SiteAdvisor*. http://www.siteadvisor.com/, 2007.

[261] L. Sloane, "Orwellian dream come true: A badge that pinpoints you," *New York Times*, p. 14, 1992.

[262] A. D. Smith and F. Offodile, "Information management of automatic data capture: An overview of technical developments," *Information Management and Computer Security*, vol. 10, no. 3, pp. 109–118, 2002.

[263] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quart*, vol. 20, no. 2, pp. 167–196, 1996.

[264] M. Sohlenkamp and G. Chwelos, "Integrating communication, cooperation, and awareness: The DIVA virtual office environment," in *Proceedings of CSCW 94*, pp. 331–343, Chapel Hill, NC, USA: ACM Press, October 1994.

[265] X. Song and L. J. Osterweil, "Toward objective, systematic design-method comparisons," *IEEE Software*, vol. 9, no. 3, pp. 43–53, 1992.

[266] S. Spiekermann, "Perceived control: Scales for privacy in ubiquitous computing," in *Proceedings of Conference on User Modeling — UM'05*, pp. 24–29, Edinburgh, UK, July 2005.

[267] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior," in *Proceedings of ACM conference on electronic commerce* (*EC 2001*), pp. 38–46, Tampa, Florida, October 2001.

[268] S. Spiekermann and H. Ziekow, "RFID: A 7-point plan to ensure privacy," in *Proceedings of 13th European Conference on Information Systems*, Regensburg, Germany: ECIS, May 2005.

[269] C. Spinuzzi, "A Scandinavian challenge, a US response: Methodological assumptions in Scandinavian and US prototyping approaches," in *Proceedings of SIGDOC'02*, pp. 208–215, Toronto, Ontario, Canada: ACM Press, October 20–23 2002.

[270] J. Stasko, D. McColgin, T. Miller, C. Plaue, and Z. Pousman, *Evaluating the InfoCanvas Peripheral Awareness System: A Longitudinal, In Situ Study.* Technical Report GIT-GVU-05-08, GVU Center/Georgia Institute of Technology, Atlanta, GA, USA, March 2005.

[271] G. J. Stigler, "An introduction to privacy in economics and politics," *Journal of Legal Studies*, vol. 9, 1980.

[272] L. J. Strahilevitz, "A social networks theory of privacy," *University of Chicago Law Review*, vol. 72, p. 919, 2005.

[273] A. Sutcliffe, "On the effectuve use and reuse of HCI knowledge," in *Human-Computer Interaction in the New Millennium*, (J. M. Carroll, ed.), pp. 3–29, ACM Press, 2000.

[274] L. Sweeney, "K-anonymity: A model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[275] L. Sweeney, "Protecting job seekers from identity theft," *IEEE Internet Computing*, vol. 10, no. 2, 2006.

[276] K. P. Tang, P. Keyani, J. Fogarty, and J. I. Hong, "Putting people in their place: An anonymous and privacy-sensitive approach to collecting sensed data in location-based applications," in *Proceedings of Conference on Human Factors in Computing Systems: CHI 2006*, pp. 93–102, Montréal, Québec, Canada: ACM Press, New York, NY. http://doi.acm.org/10.1145/1124772.1124788, 2006.

[277] P. Tarasewich and C. Campbell, "What are you looking at?," in *Proceedings of SOUPS 2005*, Pittsburgh, PA, USA: ACM Press, 2005.

[278] T. Terrell and A. Jacobs, "Privacy, technology, and terrorism: Bartnicki, Kyllo, and the normative struggle behind competing claims to solitude and security," *Emory Law Journal*, vol. 51, no. 4, pp. 1469–1511, 2002.

[279] Treasury Board of the Government of Canada, Privacy Impact Assessment Policy http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp, 2002.

[280] J. Trevor, D. M. Hilbert, and B. N. Schilit, "Issues in personalizing shared ubiquitous devices," in *Proceedings of Ubicomp 2002*, pp. 56–72, Göteborg, Sweden, 2002.

[281] S. Trewin, "Configuration agents, control and privacy," in *Proceedings of 2000 Conference on Universal Usability*, pp. 9–16, Arlington, VA, USA: ACM Press, 2000.

[282] J. C. Tullio, *Exploring the Design and Use of Forecasting Groupware Applications with an Augmented Shared Calendar.* Atlanta, GA, USA, http://etd.gatech.edu, 2005.

[283] United States Department of Health Education and Welfare, *Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems.* Technical Report, 1973.

[284] United States Electronic Communications Privacy Act of 1986 in *USC*, 1986.

[285] United States Health Insurance Portability And Accountability Act in *USC*, 1999.

[286] United States Video Voyeurism Prevention Act in *USC*, 2004.

[287] US Department of Health and Human Services, *Health Insurance Reform: Security Standards; Final Rule*, 2003.

[288] H. R. Varian, "Economic aspects of personal privacy," in *Privacy and Self-Regulation in the Information Age*, (NTIA, ed.), US Department of Commerce, 1997.

[289] V. Venkatesh, "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information Systems Research*, vol. 11, no. 4, pp. 342–365, 2000.

[290] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, no. 3, pp. 425–478, 2003.

[291] T. Vila, R. Greenstadt, and D. Molnar, "Why we can't be bothered to read privacy policies — Models of privacy economics as a lemons market," in *Proceedings of 5th International Conference on Electronic Commerce*, pp. 403–407, Pittsburgh, PA, USA: ACM Press, 2003.

[292] L. Wainfan and P. K. Davis, "Virtual collaboration: Face-to-face versus videoconference, audioconference, and computer-mediated communications," in *Enabling Technologies for Simulation Science VIII. Proceedings of the SPIE*, (D. A. Trevisani and A. F. Sisti, eds.), pp. 384–398, SPIE–The International Society for Optical Engineering, 2004.

[293] D. Walton, "Plausible deniability and evasion of burden of proof," *Argumentation*, vol. 10, pp. 47–58, 1996.

[294] R. Want, A. Hopper, V. Falcão, and J. Gibbons, "The active badge location system," *ACM Transactions on Information Systems*, vol. 10, no. 1, pp. 91–102, 1992.

[295] J. Wardell, "LexisNexis breach may be worse than thought," *AP Financial Wire*, April 13, 2005.

[296] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Review*, vol. IV, no. 5, 1890.

[297] E. Wasserman, "Here, there and everywhere," *San Jose Mercury News*, p. 1F, 1998.

[298] H. Weber, "U.S. trade commission fines data warehouser ChoicePoint over data breach," *Associated Press Worldstream*, January 26, 2006.

[299] D. Weirich and M. A. Sasse, "Pretty good persuasion: A first step towards effective password security for the real world," in *Proceedings of New Security Paradigms Workshop 2001*, pp. 137–143, Cloudcroft, NM: ACM Press, September 10–13 2001.

[300] M. Weiser and J. S. Brown, *The Coming Age of Calm Technology.* Springer-Verlag: New York, 1997.

[301] A. Westin, "Opinion surveys: What consumers have to say about information privacy, S.o.C: The House Committee on Energy and Commerce, Trade, and Consumer Protection," http://energycommerce.house.gov/107/hearings/0508200/Hearing209/westin309.htm, 2001.

[302] A. F. Westin, *Privacy and Freedom.* New York, NY: Atheneum, 1967.

[303] A. F. Westin, ed., *Information Technology in a Democracy.* Cambridge, MA, USA: Harvard University Press, 1971.

[304] A. F. Westin, *Harris-Equifax Consumer Privacy Survey 1991.* Technical Reports, Equifax Inc., Atlanta, Georgia, 1991.

[305] A. F. Westin, *E-commerce and Privacy: What Net Users Want.* Technical Report, Privacy and American Business, Hackensack, NJ, 1998.

[306] T. Whalen and K. M. Inkpen, "Privacy and security awareness: Gathering evidence: Use of visual security cues in web browsers," in *Proceedings of 2005 Conference on Graphics Interface GI '05*, pp. 137–144, Canadian Human-Computer Communications Society, May 2005.

[307] L. Wheeler and H. T. Rois, "Self-recording of everyday life events: Origins, types, and uses," *Journal of Personality*, vol. 59, no. 3, pp. 339–355, 1991.

[308] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proceedings of 8th USENIX Security Symposium*, 1999.

[309] M. S. Wogalter, *Handbook of Warnings.* Lawrence Erlbaum Associates, 2006.

[310] G. Wolf and A. Pfitzmann, "Empowering users to set their security goals," in *Multilateral Security in Communications Technology, Infrastructure, Econ-*

omy, (G. Müller and K. Rannenberg, eds.), pp. 113–135, Addison-Wesley Longman Verlag GmbH, 1999.

[311] T. Z. Zarski, "“Mine Your Own Business!” Making the case for the implications of the data mining of personal information in the forum of public opinion," *Yale Journal of Law and Technology*, vol. 5, no. 2002/2003, pp. 1–54, 2002.

[312] K. Zetter, "CardSystems' data left unsecured," *Wired News*, http://www.wired.com/news/technology/0,1282,67980,00.html, 2005.

[313] P. Zimmermann, *PGP User's Guide.* MIT Press, 1994.

[314] A. Zugenmaier, "The Freiburg privacy diamond," in *Proceedings of Global Telecommunications Conference 2003 GLOBECOM '03*, pp. 1501–1505, IEEE, 10.1109/GLOCOM.2003.1258488, December 1–5 2003.

[315] M. E. Zurko and R. T. Simon, "User-centered security," in *Proceedings of New Security Paradigms Workshop NSPW 1996*, pp. 27–33, IEEE Press, 1996.