PRIVACY AND PROPORTIONALITY

A Dissertation
Presented to
The Academic Faculty

by

Giovanni Iachello

In Partial Fulfillment
of the Requirements for the Degree
PhD in Computer Science in the
College of Computing, Interactive & Intelligent Computing Division

Georgia Institute of Technology
May 2006

PRIVACY AND PROPORTIONALITY

Approved by:

Dr. Gregory D. Abowd, Advisor
College of Computing
Georgia Institute of Technology

Dr. Warren Keith Edwards
College of Computing
Georgia Institute of Technology

Dr. Seymour Goodman
College of Computing and Sam Nunn
School of International Affairs
Georgia Institute of Technology

Dr. Paul Dourish
School for Information Sciences
University of California at Irvine

Dr. Kai Rannenberg
Chair of Mobile Commerce &
Multilateral Security
Goethe Universität Frankfurt

Date Approved: March 3, 2006

A Sarah che ha imparato la sua pazienza e me l’ha donata.

ACKNOWLEDGEMENTS

This work has significantly benefited from the help of a large group of people, at Georgia Tech, Intel Research, and elsewhere. First, in alphabetical order and for his intellectual contribution, my advisor, Gregory Abowd. Without his advice, encouragement and help, this work would not exist. I would also like to thank my committee members, Paul Dourish, Keith Edwards, Sy Goodman and Kai Rannenberg, whose pointed questions and comments greatly improved this dissertation.

I learned much from many friends and collaborators over the past few years. They made my PhD a rewarding and fulfilling experience, and helped me greatly: Sunny Consolvo, Lonnie Harvel, Gillian Hayes, James Hightower, Julie Kientz, Anthony LaMarca, Kent Lyons, Wendy March, Kris Nagel, Shwetak Patel, Jeff Pierce, Colin Potts, Tony Salvador, John Sherry, Ian Smith, Jay Summet, Molly Stevens, and Khai Truong. The members of IFIP WG9.6/11.7 “IT-Misuse and the Law” helped me by providing feedback on my early forays into ubiquitous computing security. I also thank the participants of the *Privacy in Context* workshop at Ubicomp 2005, and in particular Saadi Lahlou, Jason Hong and Günter Müller who gave advice on the design of the evaluation study.

I could have never evaluated applications without the applications themselves. Shwetak Patel and Khai Truong wrote the PAL application. Ian Smith, Fred Potter, James Howard, Jeffrey Hughes wrote the majority of the Reno application. James Scott and Tim Sohn also contributed to the Reno software. Gillian Hayes and Jehan Moghazy performed cognitive walkthroughs of the Reno application.

Zach Pousman and Lilia Moshkina went well beyond their call of duty performing expert evaluations for the Design Method Evaluaton Study. I also thank Sy Goodman, Gregory Abowd and Duke Hutchings for allowing me to recruit their students as participants for some of these studies. Finally, I thank the anonymous reviewers of the various related publications, the participants of the workshops where I discussed this work in progress and all the participants of the user studies.

Human subjects research conducted for this thesis is covered under Georgia Institute of Technology IRB approved protocols: H03221 and H03217 (PAL), H04153 (PAL Proxy), H04232 (Reno), H05055 (Proportionality Evaluation – Design Exercise) and H05187 (Design Method Evaluation Study). I thank Melanie Clark, at the Office of Research Compliance at Georgia Tech, for accommodating my tight deadlines in more than one occasion and for helping me understand the intricacies of IRB compliance.

Financial support for this work was provided in part by the NSF Graduate Research Fellowship Program. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the National Science Foundation. Further support was provided by Intel Corporation, the MacArthur Foundation through the Sam Nunn Security Program, the President of Georgia Tech, the Dean of the College of Computing at Georgia Tech and NSF ITR grant 0121661.

Thanks to Motorola Corporation for supplying the i730 handsets used for the PAL study and to Nokia Corporation for donating some of the phones used in the Reno study.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AIF	Approximate Information Flows
C&A	Capture and Access
CSCW	Computer-Supported Collaborative Work
DHS	Department of Homeland Security (US)
DHHS	Department of Health and Human Services (US)
DPA	Data Protection Authority
E911	Enhanced 911
ECPA	Electronic Communications Privacy Act
ESM	Experience Sampling Method
EU	European Union
FCC	Federal Communications Commission (US)
FERPA	Federal Educational Rights and Privacy Act
FIPS	Fair Information Practices
FTC	Federal Trade Commission (US)
GRBAC	Generalized Role-Based Access Control
HIPAA	Health Insurance Portability and Accountability Act
IRB	Institutional Review Board
IT	Information Technology
LBS	Location-Based Service
MIS	Management Information Systems
OECD	Organization for Economic Cooperation and Development
PAL	Personal Audio Loop
PET	Privacy-Enhancing Technology

PI	Personal Information
PKI	Public Key Infrastructure
QOC	Questions Options Criteria
RFID	Radiofrequency Identification
SE	Software Engineering
TTP	Trusted Third Party
UCD	User-Centered Design
VMS	Video Media Space

SUMMARY

Over the past several years, the press, trade publications and academic literature have reported with increasing frequency on the social concerns caused by ubiquitous computing—Information Technology (IT) embedded in artifacts, infrastructure and environments of daily life. Designers and researchers of ubiquitous computing (ubicomp) technologies have spent considerable efforts to address these concerns, which include privacy and data protection issues, information security and personal safety. Yet, designing successful ubicomp applications is still an unreliable and expensive endeavor, in part due to imperfect understanding of how technology is appropriated, the lack of effective design tools and the challenges of prototyping these applications in realistic conditions.

I introduce the concept of proportionality as a principle able to guide design of ubiquitous computing applications and specifically to attack privacy and security issues. Inspired by the principle, I propose a design process framework that assists the practitioner in making reasoned and documented design choices throughout the development process. I validate the design process framework through a quantitative design experiment *vis-à-vis* other design methods. Furthermore, I present several case studies and evaluations to demonstrate the design method's effectiveness and generality. I claim that the design method helps to identify some of the obstacles to the acceptance of ubiquitous computing applications and to translate security and privacy concerns into research questions in the design process. I further discuss some of the inquiry and validation techniques that are appropriate to answer these questions.

CHAPTER 1

INTRODUCTION

1.1 Motivation

Starting around the 1970's, artifacts and environments of everyday use have been increasingly embedded with Information Technology (IT)—computation and telecommunications capabilities that have enabled more elaborate behaviors and operation modes. This trend, made possible by the convergence of miniaturization and increases in computational power and energy-efficiency, has been recognized by the computer science community since the early 1990's, when Mark Weiser spelled out the vision of Ubiquitous Computing (herein called simply *ubicomp* following the community's custom[1]). According to Weiser's vision, in the future, people would increasingly be surrounded by large numbers of 'intelligent' artifacts—making computing, in fact, ubiquitous [178].

Today, this vision is becoming reality, and the collection and use of information about people and their environments is raising far-reaching organizational, social and institutional concerns, including concerns relating to information security and privacy.[2]

[1] A note on my use of the term 'community:' unless otherwise specified, I use the term community to reference the extended ubiquitous computing community roughly represented by the attendees of conferences such as the International Conference on Ubiquitous Computing, the International Conference on Pervasive Computing, the International Conference on Human Computer Interaction with Mobile Devices and Services, the International Conference on Mobile Systems, Applications and Services, the IEEE International Conference on Pervasive Computing and Communications, *etc.*

[2] In this thesis, I will consistently talk about security and privacy as two facets of the same concept. Traditionally, information security has been defined as the protection of

Early signs of these concerns have surfaced repeatedly over the past few years not only in trade publications but also in the press, as shown by the heated debate on Closed-Circuit Television surveillance (CCTV) [61, 140, 173], the risks associated with Radiofrequency Identification (RFID) technology in consumer goods [70], and the debate on positioning technology in the Enhanced 911 (E911) system.[3]

The ubicomp research community has long recognized that these are not just engineering concerns, but represent formidable challenges to adoption. Furthermore these technical developments may present undesirable side effects that require researchers and manufacturers to exercise their professional and ethical judgment. In a historical perspective, these issues are hardly novel: the introduction of automatic data processing in the 1960's raised similar concerns over control and accountability in the processing of information (both related to security and privacy). These concerns prompted far-reaching action, such as the enactment of data protection and computer security Acts in Europe and the United States and the development of professional codes of ethic, such as ACM's and IFIP's [23, 35]. What is arguably different today, is the amount and quality of collected information, which have changed vastly over what was possible in the 1970's, and the automatic and unsupervised operation of many ubicomp applications. Existing technical,

the "confidentiality, integrity and availability" of information and information services [50]. There is no such straightforward, agreed-upon definition of privacy, in part due to the heated policy debate around this concept. For the purposes of this thesis, I will adopt the concept of security and privacy suggested by *multilateral security* [153]. According to multilateral security, privacy and security define potentially competing requirements on the confidentiality, integrity, availability and accountability of information with respect to multiple parties. The use of the word 'privacy' in this context should not be confused with the concept of *personal privacy* that I use in opposition to *data protection*.

[3] Enhanced 911 is a program of the US Federal Communications Commission that requires operators of wireless phone service to locate the customer's handset in case of emergency calls with a high degree of accuracy $(< 100m)$. See http://www.fcc.gov/911/enhanced

organizational and legal frameworks for protecting information security and privacy may not be adequate in this new landscape.

1.1.1 The Response of Computer Science Researchers

The automatic collection, processing and storage of large amounts of data engender worries about the uses or abuses of such information, which may cause economic harm, disrupt established social practices or affect technology adoption. In response to these concerns, several research groups in the ubicomp community have attempted to address security and privacy issues arising from ubicomp applications, both by examining individual applications (*e.g.*, Boyle *et al.*'s work on a privacy-sensitive web cam [38]), and by suggesting general design approaches (*e.g.*, Jiang *et al.'s* Approximate Information Flows analysis framework [110]).

Although reflections on specific applications and mistakes typically have been well received, general 'design methods'[4] and guidelines addressing security and privacy have met the skepticism of the research community and of industry. Such lukewarm reception may be due to several factors, including the lack of prescriptive power of these methods for a diverse range of applications, their perceived cost in the overall design process, the lack of a design process model to situate them and an unclear definition of the target audience for these methods. Whatever the reason, the lack of follow-up to, let

[4] A note on terminology: in this thesis, *design method* indicates a general process for solving design problems in the context of security and privacy (*e.g.*, follow a certain set of steps). *Design technique* indicates a specific tool used in accomplishing part of the design task (*e.g.*, a user survey). *Design guidelines* are rules-of-thumb with pre-defined suggestions on how to tackle design problems (*e.g.*, minimize information collected). *Design frameworks* propose a certain way of segmenting and decomposing the design space (*e.g.*, look at information flows between individual users).

alone adoption of, these techniques both within the research groups that published them and in the ubicomp community at large is striking.

This is not to say that no progress has been made. Over the past 10 years, the discourse around security and privacy in ubicomp has become increasingly refined. After initially discussing generic threats to the users of these applications, researchers concentrated on specific concerns raised by practical ubicomp applications, such as location systems and video-communications in office environments (for example, the work at EuroPARC and Olivetti Research in the late 1980's). Often, reflection on these deployments resulted in specific design guidelines (a classic example of this is the work of the early 1990's by Bellotti and Sellen [31]). As understanding of specific applications progressed, others have attempted to translate security and privacy principles originating from different disciplines to the domain of ubicomp design. For example, in an often-cited theoretical paper of 2001, Marc Langheinrich attempted to expose the implications of the Fair Information Practices (FIPS), a widely known set of data protection principles used in IT, on the design of ubicomp systems [116].

More recently, several authors have pointed out that concepts deriving from economics and social sciences may be applied to understanding users and thus defining requirements in this domain. For example, Jiang *et al.* have proposed employing economic theories to evaluate transactions based on the value that knowledge and information have in making optimal security choices [110]. Palen and Dourish, among others, have pointed out how the social sciences can help in the understanding of behaviors people adopt when modulating their personal 'privacy boundaries' in interpersonal relations [143]. This work is significant because it suggests that the traditional approaches of computer scientists to these problems (adding security functions to applications, restructuring communications networks, *etc.*) may not be sufficient to solve the security and privacy challenges of ubicomp applications. In fact, there has been much work by systems and networking researchers focused on providing technical solutions to actual or perceived privacy and security problems, but few real-world applications, if any, have been able to satisfy all security requirements using technology alone.[5]

1.2 Problem Statement

Motivated by the above considerations, I started to explore whether it is possible to provide designers with more effective and general tools to address security and privacy concerns in a structured and systematic way. Specifically, I am interested in enabling designers[6] to be more responsive to user needs and social policy, by performing better assessments of emergent uses and acceptance problems and exert effective influence on the security and privacy properties of ubicomp technologies *during development*.

In light of these concerns and the lack of adoption of these general techniques, I am interested in providing tools for improving the design of ubicomp applications as well as aiding those in charge of deploying them in research environments or in real-world settings. One contribution to solving these problems is by proposing a design method for ubicomp applications that focuses on security and privacy. This is not the only way that these problems can be addressed: policy intervention, education efforts aimed at increasing awareness of novel technologies among the public, industry cooperation for devising best practices, and developing adequate management and organizational structures all contribute to the same goal. In fact, all these interventions may be necessary to increase

[5] In fact, it is ironic that some of the most advanced security and privacy technologies (*e.g.*, Public Key Infrastructure, Anonymity Networks), built to change the "distribution of trust" that is necessary to achieve application goals, require increasingly sophisticated social and organizational support structures to redistribute such trust.

[6] A clarification on the definition of designers: this work is currently targeted at the ubicomp research community, which is composed of a mix of engineering sub-disciplines, including systems, networking, and human-computer interaction. While I have tried to make this work appealing for the industrial development community, I did not engage in a dialog with that community that would allow me to claim that this work could be adopted by them in its current format.

technology acceptance. In proposing a design method, it is necessary to understand why the success of previous design methods has been limited. I claim that this lack of success is in part due to a disconnect between design and users and to a perception that design methods are costly and unnecessary.

1.2.1 Disconnect Between Design and Users

First, security and privacy have been approached, by the research community, in an absolute way, disjoint from each other and from the manifold concerns of the broader socio-technical and economic environment. The debates over CCTV, RFID and E911 cited in the opening section suggest that achieving adequate security and privacy is in fact embedded in a broader discourse of evolving dynamics related to purposefulness, fairness, and appropriateness in social relations. Recent sociological theories (such as that of Latour’s socio-technical hybrids [118]) highlight the integrated nature of socio-technical evolution. Even in the ubicomp literature, accounts of deployments of applications such as video awareness systems [31] or location technology [176], indicate that privacy subsumes a system of stakeholder concerns, including power balances, social relations and knowledge, which reflect the evolving dynamics mentioned above. These dynamics are not always made explicit during design and development, because they are hard to express in terms of technological design choices.

Cultural circumstances have a strong impact on design practice as well. Assessments over what constitutes a threat to privacy or what is appropriate conduct in mediated communication vary over time and across social, organizational and cultural contexts [21]. Even cultures that share much, both socially and technologically, like Western Europe and the United States, have different perceptions that are reflected, for example, in quite different stances on the need for data protection, and in different legislative and organizational measures for addressing these challenges.[7]

Furthermore, IT security has traditionally been considered antagonistic with usability: an entire line of research in usable security demonstrates the difficulty of managing and operating all kinds of IT security functions [156, 187]—from personal encryption tools [182], to usability of network administration interfaces [27] and software updates [148]. These problems are in part caused by unripe understanding of the use of the technology in everyday settings and misleading risk analyses, as detailed by Grinter *et al.* [80].

User perceptions of security are as important as the actual usability of the security functions of an application or system. For example, website usability has been indicated as one of the determining factors in the positive assessment of website credibility and trustworthiness [67]. Therefore, understanding of the users and of the context of use is necessary to understand not just emerging, actual security problems, but also users' perceptions, because both can affect adoption.

In this context, the problem of understanding the effects of novel technologies becomes central. The research community needs to produce techniques for probing the perceptions, desires and behaviors of users that are reliable, accurate and cost-effective.

1.2.2 Are Design Methods Worth The Hassle?

Lack of understanding of users and the novelty of this design space may explain in part why design methods and frameworks have been hard sells to the designer commu-

[7] This is readily observed by comparing the different scope of and the role of government in US data protection legislation, such as HIPAA [10] and FERPA [9], with EU Data Protection Directive 95/46 [1], the UK Data Protection Act [7] and the German Federal Data Protection Act.

nity. However, proponents of design techniques or approaches must consider numerous inherent issues as well. Perceived effectiveness is a primary concern because demonstrating the effectiveness of a design method, in terms of the increased number and quality of design features or problems solved, is a very difficult proposition. As far as I am aware, very few design methods or frameworks for security and privacy have been validated in the context of ubicomp design. Even if validation were to occur, cost considerations may kill any such proposal. In a recent workshop, Saadi Lahlou (responsible for the development of an experimental ubiquitous "office memory" project at Electricité De France's Laboratory for Design for Cognition) commented that security guidelines are unhelpful to designers because they are often negative in nature (*e.g.* "allow access on a need-to-know basis") and thus represent roadblocks to design, instead of facilitating it.[8] Lahlou further suggested that expressing guidelines in positive terms might be more useful to designers.[9] This comment, made as a sideline to a privacy workshop, captures the point of the problem. The design of new technologies is a complex, expensive and often idiosyncratic process, which relies on trade knowledge and established practices as much as on individual ability of the designer. Therefore, attempts to prescribe additional steps or analysis requirements incur a natural resistance. Coupled with doubts about the effectiveness of the design methods proposed to date, cost considerations make adoption of novel design techniques a rarity.

[8] September 11th, 2005. Workshop "Privacy in Context" at Ubicomp 2005. This is my recollection and interpretation of Lahlou's words.

[9] Patterns offer such positive guidance, but suffer from being difficult to generate in young design domains such as this.

1.3 Thesis Statement

The thesis statement is preceded by three definitions. The six thesis claims are evaluated in Chapter 5.

Definitions

Proportionality design method: a design method intended to aid the design of secure and privacy-preserving ubiquitous computing applications, based on the evaluation of the desirability of application goals, the appropriateness of the technological implementation and the qualities of salient aspects of the application interface and information policies.

Generality across individuals of the proportionality method: the structure of the design process and the research questions suggested by the proportionality method are independent of the individual applying it.

Acceptable cost of the proportionality method: applying the proportionality design method causes at most an acceptable increase of design and development costs (in terms of design time) compared similar design tasks done without the method.

Thesis

The proportionality design method 1) can be employed in the design of ubiquitous computing applications, to 2) support requirements analysis by indicating pertinent research questions targeted at improving the understanding of applications and their usage context; 3) select the most appropriate alternative among design options, 4) in a way that is general across individuals, 5) carries acceptable cost and 6) leads to identify more privacy and security issues—and more relevant issues—compared to other similar design methods.

1.4 Contribution

In this thesis, I argue that the scope and complexity of people's motivations and behaviors, cultural and temporal differences in the adoption of IT, the rapid change of technology, and structural issues with design practice are some of the reasons why a general understanding of the acceptance of ubiquitous computing applications and systems eludes us and design techniques targeted at solving the related security and privacy problems lack adoption.

As discussed in the preceding paragraph, design methods are not enough for gaining a comprehensive understanding of the problem and the users, and are, at any rate, difficult to impose on designers. These two points have driven the research efforts documented in this thesis. To address them, I propose a design method that focuses on generating *design questions*, rather than a complicated procedure intended to provide *answers*. This method is complemented by individual design techniques that can be used to answer specific questions about security requirements raised upfront or later during design. Summarizing, this work contributes in two major ways to the state of the art in the field of ubicomp security and privacy. First, I propose the *proportionality method*. Second, I show how this method can be used within an experimental procedure.

1.4.1 Design Method

The proportionality method is based on salient questions inserted in an iterative design process, complemented by practical suggestions on how to use it. Specifically, the purposes of this design method are to:

– structure the design and evaluation process of the privacy- and security-related aspects of the ubicomp application or system; and

– support compelling arguments about the quality of the resulting design.

In view of the current published literature, this method constitutes a valuable contribution to the research in the field. The proposed design method can provide useful guidance to designers and is more attuned than other surveyed design techniques to current design and evaluation practices, as conducted both in the industry and in the legal and DPA communities. The design method is introduced in Chapter 4 and its evaluation is presented in Chapter 5.

1.4.2 Design Tools and Practical Application

The proportionality method itself is similar to a scaffolding structure, in that it provides a framework for organizing the design of ubicomp applications, in terms of balancing competing needs with security and privacy concerns. However, it does not prescribe how to conduct such design in practice.

The second contribution of this work is the application of the proportionality method in practice to inform the development of new applications. I discuss some design and evaluation techniques to address the security and privacy issues induced by ubicomp applications, and of how to integrate these techniques within a larger design process.

In Chapters 4 and 6, I examine the relative merits of different techniques, how to define questions deriving from the proportionality method into questions amenable to be researched in user studies, and the integration the results back into a global proportionality evaluation.

I do not intend to provide an exhaustive discussion of user-centered design for ubicomp security and privacy. Rather, I offer examples of how targeted user studies can answer to specific, relevant questions raised by the design method and the results can be fed back into the design process. In this process, designers can select what aspects of the design they want to address without committing to a complex framework.

1.5 Roadmap

This thesis is divided in seven chapters.

Chapter 2 introduces the normative and social context of security and privacy as it relates to ubicomp technology.

Chapter 3 surveys existing approaches for designing for security and privacy in the context of multilateral security and user-centered design.

Chapter 4 describes the proportionality design method and its relationship with User-Centered Design and Multilateral Security. It also describes its application to two case studies, a personal memory aid called the Personal Audio Loop and a location-enhanced person-finder called Reno.

Chapter 5 documents the evaluation of the design method, including the pilot study performed in the Spring of 2005 and the design method evaluation conducted in the Fall of 2005.

Chapter 6 documents three design tools that I have used over the past few years to tackle specific privacy questions in mobile and ubiquitous applications: one diary study and one survey regarding the Personal Audio Loop; and the deployment study of Reno.

Chapter 7 concludes by reviewing design principles, guidelines and design methods as complementary instruments. It also synthesizes some challenges facing ubicomp development, including ubicomp security management.

CHAPTER 2

THE SOCIAL AND NORMATIVE CONTEXT OF SECURITY AND PRIVACY IN UBIQUITOUS COMPUTING

This chapter and the next provide background information and a discussion of related work. The present chapter includes some social and normative issues that affect privacy and security in ubicomp and that have motivated and influenced the development of the proportionality method. The next chapter contains an overview of the most relevant related work in the technical literature, specifically focusing on how the ubicomp community approached privacy and security issues within the design process.

This chapter is organized around several observations and comments on specific issues of interest. In Section 2.1, I claim that the complexity of ubicomp systems, their pervasiveness and interrelationship with social practices require designers to approach the development of new technology with heightened attention to and scrutiny of the potential implications of the technology. I also point out that many observers have recognized that technological evolution does not always follow causal patterns.

In Section 2.2, I propose a characterization of privacy that is slightly different from the typical characterizations used in the ubicomp community. This characterization of privacy is used throughout this dissertation.

In Section 2.3, I describe some aspects of the debate around privacy and surveillance that are particularly interesting for this thesis because some of the applications considered in this work directly resemble surveillance systems.

Finally, in Section 2.4, I point out the importance of considering security and privacy management at the time of design; this theme has been overlooked by much ubicomp research due to various reasons and I believe it will become increasingly important in the near future.

2.1 The Need for Comprehensive and In-depth Analysis

Personal **privacy** has represented a concern in the ubicomp research community from the very beginnings of the field [178]. The rapid development of IT between 1960 and 2000 has highlighted the risks caused by the changing technological landscape, such as new crimes enabled by the collection of personal information (*e.g.*, identity theft, misuse of personal health information). Understandably, the development of ubicomp applications has caused concern in the research community and among IT manufactures, motivated both by the risk of acceptance failure (thus undermining manufacturers' and service providers' revenue), as well as by the potential social and economic liabilities of ubicomp systems, and by their impact on society.

Information **security** has also come increasingly to the forefront as a topic of research in ubicomp. This interest is in part fueled by high-profile security problems afflicting present-day networked systems, especially on public networks such as the internet (viruses, email scams, worms, *etc.*). The concern is that these problems may also plague future ubicomp systems, with the added complexity of ubicomp systems' automatic, unsupervised and largely un-auditable operation. Moreover, ubicomp technology often interfaces with the physical world (*e.g.*, actuators controlled by computing devices) and may thus introduce further risks.

To understand how high-level security and privacy concerns relate to the goals of designers, we must analyze them within the broader picture of the discourse within the legal, regulatory and design communities, as well as within society at large.

2.1.1 Stating the Case for a Preventive Attitude towards Technology

In this changing and unstable landscape, designers cannot afford to ignore social and legal constraints in IT design. Not only do legal requirements and social concerns have direct and significant consequences on technology design, but in-depth knowledge of these concerns may help prevent costly mistakes.

In a recent special issue of *Human and Ecological Risk Assessment* prepared by a Swiss Federal Laboratory and dedicated to ubicomp, Claudia Som *et al.* argue that developers of potentially disruptive technologies such as those in ubicomp should adopt a preventive attitude towards technical development [159]. As a guiding principle, they propose the Precautionary Principle, which is used to perform policy determinations with strong unknowns at the national and international levels (*e.g.*, policy decisions involving the natural environment). They argue that designers must consider two kinds of uncertainties in technical development: uncertainties about the acceptance of technology and uncertainties about its social, health and environmental impact.

Designers might not be in the position of deciding on these issues—in many cases they rest in the hands of policymakers, courts and Data Protection Authorities (DPA), with the final judge being market acceptance. However, I believe that designers need to address these issues, if for no other reason than to increase profitability and hedge industrial liability. Increasing designers’ awareness of the motivation and potential impact of novel computing systems may contribute to development patterns that are less technology-driven and oriented instead towards users’ and stakeholders’ needs. This focus on user needs is one of the driving motivations for the proportionality method and will be discussed in more detail below.

Understanding these issues is not a straightforward task, and to avoid naïve conclusions, it is necessary to state clearly the boundaries of the arguments within this thesis. In addition, motivations, causes and consequences of socio-technical development cannot be viewed in a mechanical manner. To illustrate these difficulties in practice, I will cite three issues which designers should keep present while designing and testing ubicomp technologies. These closely related issues include the contradictory effects of technical development; the co-evolution of social practice and technology; and the contradictory effects of legislation on technical development.

2.1.2 The Contradictory Effects of Technical Development

A general point worth mentioning is the potentially contradictory effects that technology can have on social practice. The same artifact may produce apparently opposite consequences. For example, Arnold argues that cell phones both increase social connectedness, by enabling distant friends and acquaintances to talk more often and in a more unplanned way than previously possible, and also raise barriers between physically co-present individuals, creating, so to speak, "bubbles" of private space even in a very public and crowded space such as a train compartment [22].

Giddens writes in similar terms when he lists the "dilemmas of the self" brought on by mediated communications [76]. According to Giddens, modern technology has both a unifying and fragmenting effect on social practices: it unifies people and events happening in distant corners of the world, while fragmenting individuals who may share a common physical space but be engaged in highly individual activities that exclude the other people present.

Giddens' work is very broad, encompassing social structures, power organizations and the marketplace. Considering all these aspects would not fit with the scope of the present work. However, his work suggests that effective analysis of novel technology must proceed along multi-dimensional lines, and it must consider potentially conflicting effects. In this perspective, ubicomp design becomes an exercise of systematically reconciling potentially conflicting effects of technologies and, implicitly, conflicting needs of the stakeholders.

2.1.3 Socio-Technical Co-evolution

In the past few decades, many ubicomp technologies have enjoyed mass adoption within a rapidly changing social and normative landscape. The introduction of ever more sophisticated applications (*e.g.*, location technology based on cell phones, portable cameras) happened alongside the gradual introduction of legislation aimed at regulating their use [3, 8, 12]. At the same time, heightened awareness of information security risks has prompted legislation requiring certain measures of information security in certain domains, such as healthcare, financial services and corporate governance [11, 66, 174].

Legislation may be viewed as a symptom of the need to curtail actual or potential abuse, while granting legal status to mainstream uses of a technology or application. In such a model, legislative change occurs after a technology has begun penetrating the marketplace. As such, it follows, in part, the evolution of social norms and practices, which change based on technical development. On the other hand, there are many cases of existing legislation influencing technical development. In some cases, specific legislation has even been enacted preempting technical development. For example, digital signature legislation in European countries was enacted well before the technology reached mass-market. Some argue that this preemptive legislation may have in fact slowed development and adoption.

It is often difficult to tease cause and effect apart: whether legislation and legal case history or social practices drive the development of technology or vice-versa. Many observers have noted that the relationship between social constructs and technology can be better described as *co-evolution*. For example, Latour talks of socio-technological hybrids, undividable structures encompassing technology as well as culture—norms, social practices and perceptions [118].

It is not in the scope of the present discussion to describe the co-evolution of social norms and technology, a task best left to sociologists and philosophers. However, where appropriate, I will point out the relationship between social and legislative structures and a technological instance.

2.1.4 Interpreting Legislation

The scope and frequency of regulatory action in the IT domain has greatly increased over the past 30 years, to the point that it is impossible today to ignore legislation in ubicomp design. In the context of this thesis, it is particularly interesting to study how courts have interpreted legislation in practical cases. Below, I briefly overview specific cases in which privacy legislation was interpreted and applied by Data Protection Authorities and Courts.

2.1.4.1 The Role of DPAs in Interpreting Regulation

A vast body of knowledge regarding the impact of technology on individual privacy rights has grown over the past century in rulings and opinions issued by courts and, more recently, Data Protection Authorities (DPA)—supervisory entities with regulatory, oversight, ombudsman and enforcement powers on data protection matters.[10] In fact, some regulators have interpreted existing legislation for new technology. Their work offers interesting insight to designers for understanding where regulatory and legislative efforts are headed. In the past few years, the data protection community in Europe has been active with regards to video,[11] telephone and email surveillance in workplaces [163]

[10] DPAs are sometimes called Information Commissioners. In the United States, the FTC, the DHHS and the DHS are assigned some of the responsibilities of European DPAs within specific regulatory frameworks (respectively, internet privacy policies and financial regulation, HIPAA, law enforcement databases). For example, the FTC regulates the financial sector in connection to the Gramm-Leach-Bliley Act and other regulation, and leads enforcement activities related to privacy policies for internet web sites.

[11] Surveillance technology is used in this thesis as a benchmark because it is representative of both the technical properties and information flows of many ubicomp systems

and CCTV systems in public space [171]. In the United States, the governmental agencies' leeway in interpreting regulation dealing with privacy is more limited. For example, the FCC has maintained a relatively hands-off approach on the management of location data from cell phones.

The European Commission's Article 29 Working Party (an appointed body of the European Commission that functions, roughly speaking, as an EU-wide DPA) has provided opinions on applications of automated sensing technology, *e.g.*, video surveillance on commercial premises and private dwellings [61], and biometric technology in both governmental and commercial settings [62]. In these reports, the Working Party cites examples of actions taken by national DPAs in specific cases of the application of data protection legislation, pointing out advantages and deficiencies of specific approaches. The Working Party also suggests some specific examples as best practices. For example, in the report on video surveillance, the Working Party discusses the positioning and operating modes of a surveillance camera at the entrance of an apartment. In the report, an analysis is made of how detailed design parameters (the cone of the camera, its orientation, the resolution of the resulting video) affect other dwellers and passers-by. In the US, the General Accounting Office (GAO) has published a report on the use of CCTV for surveillance of federal property in the Washington, D.C. area, analyzing the boundaries of the observed areas and the management structures behind two large surveillance operations in the capital city [173].

The British Institute of International and Comparative Law compiled a summary of DPA rulings on video surveillance across the EU [40]. These comparative studies are extremely interesting for designers of applications with cross-boundary markets because

(which collect, store and use data from environments), and because it typifies many of the risks and concerns commonly associated with ubicomp.

they bring to bear subtle differences in national contexts, even within a supposedly uniform regulatory space (the EU). In a similar way, comparative studies in the US have indicated differences across state regulations that affect the collection of information from environments, such as surveillance videos or audio recordings [150]. This literature can provide valuable advice to designers and justification for defining application parameters and operating modes.

The work by DPAs on this topic is particularly interesting because the principle of proportionality proposed in this thesis is directly inspired by their approach to privacy and security problems. For example, in the discussion of the video camera installed at the apartment entrance mentioned above, a tradeoff is made by the regulator between the need for capturing the faces of people at the door while being minimally invasive of the rest of the space around the entrance, so that unrelated individuals can walk by unobserved [61].

The need for balancing competing needs in IT has also been stated by influential scholars and observers of technology policy. In his renowned book *The Limits of Privacy*, Amitai Etzioni shows how needs for protecting collective welfare may be opposed to principled privacy concerns [60]. His arguments specifically relate to US public policy and to public uses of technology—personal ID cards, HIV testing and video surveillance, but his point can be extended to some of the ubicomp applications examined in this thesis, which have less apparent public and private benefits. Etzioni adopts a pragmatic stance towards privacy and advocates setting up a regulatory system not unlike that present in the European Union, balancing competing safety, security and privacy needs with a pragmatic, case-by-case approach in addressing privacy concerns. The theme of balancing stakeholders' needs is central to this dissertation and will be discussed further below. In fact, Etzioni's analysis routinely draws from the three questions embedded in the proportionality method—desirability, adequacy, and appropriateness.

2.1.4.2 The Role of Courts

Court rulings also provide valuable input and a baseline for this work. Although the following list is by no means comprehensive, I wish to detail three points affecting the present dissertation.

The United States Supreme Court provided opinions involving the "chilling" effects on First Amendment rights of surveillance in public space (*e.g.*, during public demonstrations) [30, p. 168]. In that case, a tradeoff was made between the protection of free speech and the need for preventing criminal activity by the use of sensing technology in public space. Similarly, in a case of illegal over-the-air wiretapping of cell phone conversation (*Bartnicki v. Vopper*, 2001, cited by Terrel and Jacobs [164]), the Supreme Court considered the tradeoff between the need for the public to learn about allegedly criminal conduct of a public official and the breach of his privacy when a cell phone conversation involving him was illegally broadcast by a radio station.

The concept of reasonable expectation of privacy in the face of rapidly improving sensing technologies has been developed by the US Supreme Court in *Katz v. United States*, 1967 [5]. This case is relevant because it provides a baseline of the court thinking concerning surveillance technologies. Although the case specifically involves Fourth Amendment rights, and thus is targeted at the relationship between individuals and government, some of the conclusions could be applied to person-to-person interaction. These opinions and rulings are not always directly applicable for our purposes and must be therefore accurately characterized and employed, in a predictive, rather than prescriptive manner.

Only recently have specific technologies been systematically analyzed by legal scholars to address the policy issues induced by them. For example, Zarski addresses the issues related to data mining, and claims that data sensed from physical environments are primary sources of risk [184]. Terrell and Jacobs discuss a case in which advanced sensing technology has been used to examine the interior of a dwelling in a criminal investigation [164]. In that case, *Kyllo v. United States*, 2001 [6], the Court argued that the reasonable expectation of privacy depends, in part, on what technology is commonly available.[12] This argument has profound impact on technological development and on adoption, because it bases the legitimate use of a technology on the knowledge that the public may have about it. This point will arise again when discussing user studies of ubicomp technology, adoption and future avenues of research.

2.1.5 The Ultimate Judge: Adoption

In the Kyllo case, legality of a technology was tied to the concept of commonly available—adopted—technology. It follows that understanding and predicting adoption patterns should concern the designer of novel technologies. Adoption is important because security and privacy requirements often are influenced by the level of acceptance and awareness that the users and the public have of a certain application. Influential authors have pointed out that understanding and predicting adoption has a significant economic impact as well.

For example, in the book *The Invisible Computer*, Norman introduces the concept of IT-centric devices that he calls 'information appliances,' single purpose, self-contained, networked, task-oriented ubiquitous computing applications (a typical example would be the Apple iPod^{TM}). He describes their development in terms of an established segmentation of product lifecycle (introduction to market, revenue generation and decline). Norman notes that different types of users (early adopters, mainstream, late adopters) relate to technologies in different ways at different stages of their lifecycle, and

[12] In the case considered, a thermal imaging sensor was used to trace heat levels emanating from a private dwelling, which suggested the presence of high-powered lamps inside the home, used for the cultivation of marijuana.

suggests that the market success of new technologies would benefit from intentionally leveraging these relationships [138]. Norman also cites information privacy as one of the threats to the widespread success of information appliances. Christensen *et al.*, in the recent book *Seeing What's Next*, propose an analytic framework for predicting market acceptance of novel technologies [44].[13]

Both books use the telecommunications industry as a case study and characterize the telephone as a disruptive technology, with profound implications on society, in a way that is strikingly similar to how ubicomp is characterized by its proponents. It is not surprising that both Norman and Christensen *et al.*, who belong to very different communities of interest (respectively, human factors and business management), assert that understanding the market is paramount to influence acceptance and that an adoption strategy must be part of the overall development strategy for new technologies.

2.1.6 Summary

The examples reported above should convince the reader of the complexity of the social context of this thesis. The obvious need for addressing security and privacy issues of ubicomp applications in a user-centered manner induces the designer to test the limits of existing normative, social and regulatory environments. Furthermore, security and privacy concerns are just some of the elements in the much wider discourse regarding the adoption of disruptive technologies. These concerns often have subtle effects, but are rarely the only or primary cause of the success of failure of a given technology.

In the remainder of this Chapter, I expand on some aspects of privacy and security that are relevant to this thesis and are rarely mentioned in the community's literature.

[13] I limit these citations to authors who have examined mass-market adoption as opposed to adoption within organizations. The MIS and CSCW communities provide numerous accounts of the latter (*e.g.*, Venkatesh [175], Markus [126]).

2.2 Characterizing Privacy

The experiences of European DPAs and Courts in the United States are very different not only in terms of the conclusions they reach, but also in the legal and constitutional underpinnings. In the present section, I explain another difference, relevant to my work, in how privacy is perceived and addressed in different societies and legal frameworks. Other authors describe various flavors of privacy (specifically, in the ubicomp community, Langheinrich [116] and Boyle and Greenberg [39]), using categories such as *Privacy as an Interpersonal Process*, *Privacy as Need, Right, Freedom*, or *Privacy as Balancing Act*. I do not intend to replicate their work and refer to these articles and to their references for more information on these useful characterizations of privacy.

There are, however, two points that are rarely stated clearly in the literature and that are important in the context of this thesis. The first relates to the perceived differences between approaches to privacy in two of the most significant markets for upcoming ubicomp applications—Europe and the United States. The second issue relates to the difference between Data Protection and Personal Privacy.

2.2.1 Europe *vs.* United States

Attitudes towards privacy are quite variable across national and cultural boundaries. A classic argument made at workshops and conferences on privacy opposes the "European" centralized, highly regulated approach to privacy with a *laissez-faire* attitude adopted in the United States, especially in relation to corporate entities collecting personal information. Proponents of this distinction note that data protection regulation is much more developed and comprehensive in Europe, following early action by individual nations, such as Germany [127] and the enactment of blanket regulation at the EU level, including EU-wide legislation (*e.g.* Directive 95/46 [1]).

Although, as a first approximation, this characterization may hold, at a deeper look, it is overly simplistic. This view does not take into account a growing case history of US court rulings on matters directly affecting privacy, the increasing calls for the enactment of privacy legislation,[14] and the voluntary initiatives directly taken by service providers, especially mobile telecommunication operators, in managing personal information deriving from mobile and ubiquitous computing systems.

In fact, the success and acceptance of technologies that resemble surveillance in workplaces and in public space, varies on factors that are more fine-grained than national legislation, such as local regulation, unions' influence, organizational culture and individuals' opinions. This is also true when considering applications for consumers outside of formal organizational structures. Consequently, analysis that takes into account only differences between regulatory regimes in different countries is too blunt to provide effective design guidance. This point arises again in the following section, when talking about design and inquiry tools for answering specific questions about privacy in design.

One example of how US data protection laws are similar to those in the EU is FERPA, the US Federal Education Rights and Privacy Act. This federal law imposes strong safeguards and access rights on the personal data of pupils collected in federally funded schools. FERPA adopts the Fair Information Practices (FIPS) and effectively constitutes data protection legislation in the style of similar European laws. The relevant difference is not between the American and the European approaches, but between data protection and personal privacy.

A symmetric argument is often made by researchers with relation to personal privacy, especially with respect to the relationship between individuals and the government. Common opinion asserts that Americans are more jealous of their personal space than Europeans, backed by strong protection originating from the US Constitution's Fourth

[14] *E.g.,* legislation like HIPAA, the Federal Wireless Act, laws protecting against identity theft, etc.

Amendment. However, the recent spread of CCTV systems in US urban areas [173] and discussion about widespread domestic surveillance [106] mirror similar trends in the European Union (*e.g.*, CCTV and telecom data retention), suggesting that US and European preferences on personal privacy, if they existed in the past, may be progressively converging.

2.2.2 Personal Privacy *vs.* Data Protection and Informational Self-Determination

A misunderstanding of the mutual relationship between personal privacy and data protection often confounds the discussion on privacy. The distinction is important not just on theoretical grounds but also for practical reasons of system design. Personal privacy relates to the way we arrange space and behavior to project a certain image of ourselves and to protect ourselves from the invasiveness of others. Irwin Altman's classic description of how people manipulate their privacy in social and physical space is a prime example of this concept. Altman characterizes personal privacy as an ongoing exercise of "setting boundaries" between the individual and the external world [20]. Altman's work is in part inspired by Goffman's work on social and interpersonal relations in small groups [77].

The second concept, data protection, relates to the management of personally identifiable information. Here, the focus is on protecting such data at a social level by regulating how, when and for what purpose data can be collected, used and disclosed. The origin of this concept stems from the work by Alan Westin and others on the Fair Information Practices [172, 180], and on the subsequent embodiment of these practices at the international level [142] and in national legislation (starting with data protection laws in Germany's State of Hessen in 1970 and Sweden in 1973 and the US Federal Privacy Act of 1974).

Both aspects of privacy have deep legal and social ramifications and both are affected by, and affect, ubicomp technology. However, their legal and ethical grounds are distinct and the techniques and methods for tackling them are very different. Data protection calls for increasing trust in the effectiveness of the organizational and regulatory environment, the state and public opinion; it applies to the relationship between individual citizens and large organizations; to use a blunt expression, the power of knowledge here lies in *quantity*. Personal privacy, instead, decreases the need for trust by reducing communication and denying access; its major influence is felt in personal, one-to-one relationships; here power lies in *intimacy*. Bruce Schneier makes a similar distinction, between *targeted attacks* to privacy and *data harvesting* [157, p. 29].

Although much discussion in the ubicomp community has addressed one side of the issue (namely physical privacy), only recently have researchers started thinking of how data protection laws already in place affect the ubicomp design space, let alone actual implementations. At a recent workshop on ubicomp privacy, Günter Müller expressed a similar point, stating that the data protection approach is about *informational self-determination*,[15] *i.e.*, allowing individuals to choose how others can use their personal information, whereas the personal privacy approach is about setting a boundary around one's "personal space" [131]. This distinction will arise repeatedly in the discussion below.

In the remainder of this section, I will explore how different actors—civil liberties organizations, Data Protection Authorities (DPAs), courts, *etc.*—have addressed their

[15] The term *informational self-determination* was first used in the context of a German constitutional ruling relating to personal information collected during the 1983 census. In that occasion, the German Federal Constitutional Court ruled that: "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the [German Constitution]. This basic right warrants [...] the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest." [13]

concerns about advanced IT, including some ubicomp applications, and how their work relates to this thesis.

2.3 The Debate on Privacy and Surveillance

One important component of many ubicomp systems is the capture of multimedia information from environments of human action. This information can be stored and made available for a variety of functions, including supporting human activity (*e.g.*, to aid the memory of specific events), for driving the operation of computing systems (*e.g.*, to support natural interaction with humans), and facilitating communication among people (*e.g.*, increasing awareness of each other when not co-located). For example, early ubicomp systems were developed for the latter purpose and used in workplaces.[16] In work environments, social dynamics may resist the introduction of technologies resembling surveillance [103]. Expectedly, much of the initial analysis of these applications drew from that of surveillance technologies, with a focus on privacy [31].

Below, I summarize part of the debate on surveillance, using the example of surveillance cameras in urban centers as case study.

2.3.1 Social Critique of Surveillance

Social critique has long highlighted the negative impact of technology on society and their co-evolving nature. The media has followed these discussions at a very high

[16] There is no specific date that marks the beginning of ubicomp as a research field—embedded systems being an example of computing devices installed in everyday artifacts long before Weiser spelled out the vision of ubiquitous computing [178]. However, some of what are now considered among early ubicomp applications, such as the RAVE system developed at EuroPARC in the late 1980’s–early 1990’s, were deployed in the context of workplaces. RAVE used audio and video feeds, among other purposes, to increase awareness of remote co-workers [72].

level, without addressing the nuances of technological and organizational details affecting the use and effects of the technology.

Surveillance technologies have been the topic of critics, legal researchers and civil liberties groups [32, 48, 145]. An interesting example is provided by the gradual evolution of the use and purposes of a set of surveillance cameras installed in central London. In this section, I do not intend to replicate the heated debate on surveillance technologies and civil liberties; rather, my goal is to show how technological and organizational developments affect the characteristics of transportation security and may affect the role of designers.

In 1993, city authorities installed CCTV cameras at all entrance points into a 1 sq. mi. area of central London (the "City") as a preventive measure. Later, additional cameras were installed to prevent and detect traffic violations; in 1996 the system of nearly 700 cameras was enhanced with automatic license place recognition, which was used for automatic violation enforcement. In 2003 the system was connected with an automatic toll collection system, also based on license place recognition [140]. Finally, in 2003, authorities revealed that the array of cameras would be used in conjunction with pattern matching technologies (occupants' face recognition) for crime prevention and anti-terrorism purposes [166].

2.3.2 Progressive Redefinition of Purposes and Feature Creep

Critics of the London surveillance system highlight a trend toward **centralization and integration** of these infrastructures. Once the physical capture network (the cameras and associated telecommunication lines) is in place, additional capture devices can be introduced inexpensively; supervisory and monitoring functions can be allocated to optimize organizational and economic constraints; the same system can be used for different purposes. In addition, critics have objected to expanding the purposes of the surveillance system; indeed, uncontrolled '**feature creep**' can result in a system very different from what was initially agreed to by stakeholders. These trends are at odds with the traditional approach of DPAs, in that their balancing assessment assumes single-purpose systems and upfront analysis. This observation will be discussed in further detail in the section on DPA practice, and when discussing some of the assumptions of the proportionality design method.

2.3.3 Automatic Operation

One of the characteristics of ubicomp technology is its unsupervised and automatic operation. This feature introduces complex and potentially opposite ramifications. **Automatically operating systems** are already in use in some countries. The Auto Incident Recording System (AIRS) developed by Northrop Grumman, for example, is deployed at intersections and stores a certain number of minutes of video prior to an event signaling a potential accident, such as a loud crash or sharp braking sound [141]. Under ordinary conditions, the system discards recordings in a loop, similar to the Personal Audio Loop application described in this dissertation. This system provides useful information without employing humans, further reducing deployment costs, but with an uncertain effect on privacy.

Automatic operation is an important element in the debate on trust in technology, which has been very active among both scholars and DPAs in the recent past [140]. Data protection law was introduced in part to reduce the risk of automatic systems taking decisions affecting individuals without human supervision. EU Directive 95/46 mandates that no decision impacting the legal rights of or "significantly affecting" a data subject should be taken solely by automatic means based on his or her personal information [1, §15]. The intent was to protect people from malfunctioning technology, by having a human in the loop for all discriminations based on collected personal information. On the other hand, recent studies have showed that video surveillance systems are particularly prone to misuse caused by wrong perceptions and preconceptions of those (very human) individuals in charge of supervising the system. For example, Norris' ethnographic study of surveillance operators in England shows that members of ethnic minorities, foreigners and people perspicuously dressed are more often targets of surveillance than typical people [140]. Critics have observed that this practice may increase the number of incidents traceable to these minorities and ignores non-minorities, effectively creating a double policing standard. Current trends in the surveillance community favor using image processing and machine learning techniques to automatically identify events requiring attention without operator intervention (*e.g.*, individuals moving erratically or loitering). Automation moves the issue of discrimination from the operator to the developer of the system, arguably facilitating policy formulation and compliance.

All this amounts to a contradictory (or ambivalent, in Arnold's words [22]) effect on privacy: automatic technology increases risks to individuals, if it takes wrong decisions without the possibility for recourse; it decreases other risks, making it simpler to define upfront, during design, specific operating policies.

2.3.4 Beyond Surveillance

Although the discussion above centers on surveillance technologies, ubiquitous computing includes other technologies that have been the topic of critical research and legislative action as well, such as location sensing [47], RFID tagging [70], and portable digital cameras [12]. Surveillance systems can be generalized in a class of technologies that is sometimes defined as *capture and access* technologies by Abowd and Mynatt [14]. This term is commonly used to indicate systems that capture information from environments of everyday action, such as video/audio feeds, store it and make it available to other applications or subjects for later consumption [169]. One of the applications discussed in this thesis, the Personal Audio Loop, can be characterized as a capture and access application. The architecture of capture and access systems proposed by Truong

[169] is interesting because it provides a general technical description of surveillance systems that can be used for systems analysis [96].

2.4 Security in the Context of Ubicomp

In this section, I briefly mention some effects of security legislation and management on ubicomp applications. I also claim that security management has not been a topic of much research in the ubiquitous computing community to date. Management concerns may not have had time to surface, given the lack of large deployments of ubicomp applications (cellular phones being one notable exception). However, the heightened awareness of security in the media and the introduction of legislation mandating security requirements should prompt researchers to consider security legislation and management as primary elements of the design process of ubicomp technology.

2.4.1 The Impact of Security Legislation on Ubicomp Technology Management

Legislation directly addressing IT security has been late in coming. Until the 1970's, security was a topic of practical concern mainly in governmental, military and large private organizations. However, recent high-profile security breaches [114, 177, 186], the increasing economic impact of security failures [65], and increased awareness among software manufacturers (*e.g.*, Microsoft [71]), have prompted the attention of the media and lawmakers. This has prompted researchers to tackle security issues in mobile and ubiquitous computing applications as well (*e.g.*, fixing security issues in 802.11 wireless networks).

Information security requirements have been introduced with legislation addressing data protection, digital signatures and corporate governance. For example, legislation on corporate accountability imposes strong security requirements on data that may affect corporate performance [11]. Legislation on electronic health-related transactions imposes security requirements on personal information [10].

Other legislation relates to telecommunications in general and thus directly affects the design of security in ubicomp systems and applications. This legislation includes telecommunication laws that safeguards users' location and transaction information (*e.g.*, EU Directive 2002/58 [3], the US Electronic Communications Privacy Act [8]) and laws on wiretapping and surveillance, which relate to the capture and safeguarding of environmentally sensed information.

In general, legislation is quite generic on the specific details of security, leaving implementation to regulation codes. For example, the Health Insurance Portability and Accountability Act of 1999 (HIPAA) indicates some general security goals, but specific guidelines are provided in the Code of Federal Regulations that has been written with the collaboration and feedback of health service providers (the entities regulated by HIPAA) [174]. The reason for this separation is to make updating technical requirements simpler, by decoupling legislation goals and general mandates from the evolving nature of technical issues. Therefore, researchers seeking legal guidance on design issues must consider implementation regulations as well as legislation.

When legislation commits to one specific technological solution, this may jeopardize its effectiveness. For example, the EU Directive 1999/93 on electronic signatures [2], while retaining a two-tier goals/implementation structure, has been criticized for suggesting one specific technological approach to electronic signatures (*i.e.*, the use of digital certificates) [26]. This criticism is particularly relevant for ubicomp development, as legislation may impose specific technological choices that may or not be optimal from a technical or user perspective.

2.4.2 Ubicomp Security Management—A Contradiction in Terms?

Information systems management currently represents one of the main challenges to IT security, and has recently gained much attention from industry and academia. Despite this trend, there are very few accounts of how advanced IT systems (such as ubicomp systems) are managed in practice, due to various reasons, including lack of experience in industry, resistance to publicize internal organizational matters, and lack of attention from the academic community.

The surveillance literature represents an exception in this landscape, and includes accounts on how CCTV systems are operated and managed on a day-to-day basis [140, 173]. However, to my knowledge there are no systematic, published accounts of how integrated surveillance systems employing advanced technology such as pattern matching are used and managed. As a result, security management in ubicomp systems is largely uncharted territory. However, the need for exploring this territory is pressing: the kind of information handled by ubicomp applications and their social setting of use suggest that these technologies will present significant security management challenges.

Standardized security management guidelines have been developed over the course of the past 30 years and have been widely adopted by organizations seeking cost-effectiveness and simplification. This trend towards standardization is visible in the publication of guidelines (*e.g.*, the Rainbow Series reports by NIST [134]), best practices (*e.g.*, the Generally Accepted Information Security Practices [102]) and international standards on the topic (*e.g.*, IS17799 [104]).

Ubicomp technologies bring a new scale to the management problem, which is already a difficult challenge for traditional computing systems such as PCs and corporate information systems. Security management typically rests on assumptions that are not necessarily verified in ubicomp systems. These assumptions include:

- sufficient resources and competent personnel to implement and overview security controls;
- user interfaces to inspect and audit system performance and operation;
- effective regulation and policy enforcement.

Whether security management standards and guidelines developed for traditional IT can be transferred to ubicomp is not clear.

Although security management is not directly within the scope of this thesis, one of the goals of the proportionality method is to provide suggestions for security management as part of the design process, thus bridging product design with post-deployment everyday use. This observation will be made again in the context of future work and when talking about “designing for management.”

2.5 Conclusions

In this Chapter, I demonstrated how legal and social forces interact with the development of ubicomp technology. This is not a one-way process: technical change causes social and legal action and legislation affects technical development. For example, given enough momentum, the designers of a new system might be able to change legislation: wireless regulation on location information being an example.

I further argued that it is important for developers of ubicomp applications to understand the process of adoption, in part because assessments used in the legal community in reference to privacy (such as “technology in common use”) are based on public awareness of technology, in part because of marketplace performance. Moreover, I highlighted the challenges facing security management in the context of ubicomp applications. In the following Chapter, I present a synthesis of some of the efforts in the technical literature.

CHAPTER 3

SECURITY AND PRIVACY IN UBIQUITOUS COMPUTING

In this Chapter, I provide a background on technical work that focuses on the design of privacy-respecting and secure ubicomp applications. In this Chapter, my goal is to develop two arguments that support my proposal of the proportionality method as a relevant and timely contribution to the state of the art in the field of ubicomp security and privacy.

First, the field of ubicomp security and privacy is still very young. It is hard to pinpoint exactly what a “secure” and “privacy-respecting” ubicomp application or system is supposed to provide in terms of security requirements or behaviors visible to the user. Except for some intuitions by the technical community and legal constraints, the issues at stake are relatively ill-defined. Consequently, I claim that prescriptive design methods may not provide as much flexibility and relevant guidance as design processes based on iterative development and repeated evaluation.

This argument points to the second part of this Chapter. That is, while there have been numerous attempts to model specific privacy and security concepts, principles and requirements, there is still a lack of understanding of user needs in specific applications and contexts. The analytic frameworks proposed in the literature reflect engineers’ understanding of the problem domain, but it is not clear to what degree they match user needs and are able to satisfy user requirements. That is, analytic approaches have not been validated in practice, and, in fact, most proposed frameworks do not indicate how to connect user experience with system analysis.

A skeptical reader may ask why security and privacy in ubicomp are challenging design problems. There are at least two arguments to address this doubt. First, there is relatively little documented experience related to the creation and the use of this type of IT applications. The most widely used ubicomp applications, such as military and logistics applications, originate from corporate R&D and are poorly documented in open literature. Research systems built in academic environments, while better documented, do not enjoy real-world adoption and represent thus an untrustworthy base for reflecting on and improving design practice. Applications of mobile phones are one notable exception to this, and, in fact, mobile telephony is used repeatedly in this thesis as a source of experience and as a benchmark. The second reason why security and privacy in ubicomp is a complex problem is that the design space is more complex than that of many other IT applications. Security and privacy refer to non-functional requirements which are difficult to verify in any given product. Furthermore, the effects of design failures in this domain are difficult to assess because they mix with the effects of cultural conditions, market acceptance, pricing, and other ill-understood socio-technical variables. Moreover, in many cases, the increasing number of computing devices and of their interaction patterns makes it difficult to trace effects back to a specific artifacts.

In the remainder of this Chapter, I summarize the most prominent technical work in the domain of ubicomp privacy and security. I then summarize some efforts of solving security and privacy issues by improving the design of ubicomp systems. In particular, I focus on:

- Early work on awareness and location systems in workplaces.
- Guidelines and frameworks (methodological frameworks, analysis tools and procedures, and modeling frameworks).
- Design and development techniques.
- Work in the security community addressing similar design problems.

3.1 Hot Issues in Ubicomp Security and Privacy

This thesis focuses on understanding what people expect from ubicomp technologies and what the security and privacy problems are, rather than providing specific solutions to these problems. However, technical solutions to security and privacy problems are one of the cornerstones of building secure and privacy-respecting ubicomp applications. Therefore, in this section, I list some technical work on the topic of ubicomp and IT security and privacy. I will not provide a complete catalog of technical work, but merely pointers to work the reader might want to survey personally for more information. The purpose is to map the most relevant themes of research in the field, not that of providing a comprehensive background. Specific technical work will be cited in the following chapters when discussing the case studies and the application of the proportionality method.

There are other good sources for overviews of this body of research. In the first two chapters of his Master's thesis, Scott Lederer provides a nice summary of research in the field, up to December 2003, focusing on how interaction with ubicomp applications can affect user privacy and security [119]. The January 2003 issue of *IEEE Pervasive Computing* magazine provides a broad overview of the general topics researchers are working on in the field. These articles include networking security work (Kitsos *et al.*), authentication methods to be used in untrusted environments and terminals (Pering *et al.*), advances in biometric authentication (Yongsheng *et al.*), and a discussion of location privacy (Beresford and Stajano, Myles *et al.*).

In 2003, Frank Stajano, a researcher at the University of Cambridge, UK, published the book *Security for Ubiquitous Computing.* In this book, he listed several technical security issues and techniques targeted at ubiquitous computing applications, including trust systems, networking security and anonymity [160]. The book is roughly divided in two sections. The first section focuses on the history of ubiquitous computing and mentions some of the most relevant work in the research community. The second part of the book discusses several advanced security techniques for addressing the three classic aspects of security—confidentiality, integrity and availability[17]—along with anonymity and authentication. Besides indicating some techniques that may be useful to solve some ubicomp security problems, Stajano was not able to provide much insight, partly due to the lack of deployment experience with real-world ubicomp applications. Although it was a commendable effort, the book was premature when it was published and, therefore, did not have a strong impact on the research community.

The proceedings of the workshops on privacy and security at premier conferences on ubicomp[18] also document work on topics ranging from secure networking to protecting location privacy. These conferences have published technical work on location privacy (*e.g.*, work by Duckham and Kulik at Pervasive 2005 [59]) as well as more user-centered research (*e.g.*, Kindberg *et al.*'s work on trust in ubicomp in e-commerce settings [111]). The problem of trust is deep and multi-faceted, because it requires to combine mechanisms for establishing trust between people and computing systems (*e.g.*, authentication mechanisms) with the social, physical and other conditions that influence trust.

A specialized conference, Security in Pervasive Computing, held in 2003 and 2005, published work on infrastructure for physical/virtual interaction, authentication, access control, information flows and location privacy. More work has been published at security, networking and systems conferences. For example, Covington has published work on generalized access control and identification [52] at the Annual Computer Security Applications Conference.

[17] "IT security means, confidentiality—prevention of the unauthorized disclosure of information, integrity—prevention of the unauthorized modification of information, availability—prevention of the unauthorized withholding of information or resources." [50]

[18] See Appendix A for a list of these conferences and workshops.

Two strands of research are particularly interesting in the context of this thesis: location privacy, which generalizes to the issue of securing context information, and capture and access applications security and privacy. Below, I discuss these two topics in more detail.

3.1.1 From Location Sensing to Context

The interest for location privacy was in part motivated by the debate caused by location-based services (LBS) and the introduction of location-based emergency systems on cell phones (E911 in the US and E112 systems in Europe). The collection and storage of location information raises a complex set of concerns and potential risks, involving individuals, service providers, telecom operators, governments and law enforcement. One obvious concern is that organized crime, corporate entities or governments may be able to reconstruct the physical whereabouts of individuals covertly or for illegitimate purposes. At the interpersonal level, the concern might be that technology enables disruptive and undesired practices, among acquaintances and between people who do not know each other (*e.g.*, stalking). Given the commercial interests involved, many researchers have concentrated on securing the use of location information. Proposed solutions to these concerns include using anonymity techniques. Networking protocols such as MIX networks and onion routing[19] have been proposed to decouple location information from the identity of the user [34]; information-theoretic approaches such as k-anonymity sets[20]

[19] MIX networks and onion routing allow communicating partners to exchange messages without revealing their identity to each other and the existence of communication to third parties [43, 79].

[20] k-anonymity is a technique that can be used to release public information, while ensuring both data privacy and data integrity [162].

have also been proposed to help modulate the disclosure of location information to achieve untraceability of location information [81].

One of the problems with solutions based on 'hard' anonymity is that in many cases the complexity of the anonymization technologies may curtail commercial viability.[21] For this reason, Trusted Third Parties (TTPs) have been proposed for acting as intermediaries in the collection and management of context information. Using TTPs to protect private information appears to be more feasible from technical and organizational standpoints, and reflects the *status quo* of current location-enhanced services. In the domain of location information, telecom operators are obviously in an advantageous position to become brokers of context (location) information. Telecom operators can manage user's relations with value-added service providers while preserving user anonymity. This point is made succinctly by Böhm *et al.* [37]. This model also strengthens the link between customer and telecom provider, with potential commercial returns for the provider. In fact, Rannenberg points out that providers can expand their brokering capabilities to include other facets of service provision, such as service payment and privacy management, effectively leading to comprehensive customer 'identity management' [151].

[21] This claim is supported by the lukewarm market acceptance of anonymity services such as ZeroKnowledge and Freenet [185]. It should also be noted that governments have attempted to test the legal limits of surveillance of privacy-enhancing technologies in several occasions (*e.g.*, early anonymous remailers like Penet.fi [89], and advanced anonymizing proxies like JAP [28]); this may have discouraged organizations and individuals from providing these services. However, tacit agreement in the privacy community is that the mere existence of advanced, albeit commercially implausible anonymity systems is more important than their widespread adoption. This is because the technical feasibility of such systems contributes to the policy debate around privacy and technology in several ways. For example, the fact that offenders may circumvent telecommunications wiretapping by governments by employing these systems helps disproving the case for increasing widespread surveillance capabilities.

The issues related to location privacy can be generalized in the problem of context sensing.[22] Context sensing is one of the main themes of ubicomp, as ubicomp systems need information about the user and the user's environment to operate autonomously and proactively. Collecting contextual information about individuals, such as the identity of devices neighboring the user's phone, engenders social and interpersonal risks similar to those mentioned above with relation to location sensing. Architectural solutions have been proposed to address these risks. For example, the ConFab system by Hong and Landay permits application designers to collect and use context data without disclosing information that can identify individuals [91]. K-anonymity has been suggested to control the disclosure of context information so that application goals can be achieved while preventing user identification [74].

As a side-note, context is not only an asset requiring protection but also a resource usable in security-relevant decisions. Covington, for example, shows how context information about the location of people in a home can be used to drive a Generalized Role-Based Access Control (GRBAC) monitor that grants or prevents access to ubicomp services (*e.g.*, denying access to the intelligent mixer to a child if a parent is not in the kitchen) [52]. Context information is used in the Trust Context Spaces framework by Robinson and Beigl for similar purposes [154]. In these cases, securing context informa-

[22] The term *context* is used in the ubicomp community to indicate information about the user's physical environment and state that can be used to drive the operation of IT applications. Dey *et al.* define context as the computing environment (available processors, devices accessible for user input and display, network capacity, connectivity, and costs of computing) the user environment (location, collection of nearby people, and social situation) and the physical environment (lighting and noise level) [55]. Other authors have suggested including also socially negotiated and historical knowledge in the definition of context [42, 57], but for the purposes of this dissertation, I will consider only the context as defined by Dey *et al.*

tion requires the designer to consider the classic problems associated with protecting security infrastructure, including ensuring reliability and integrity.

3.1.2 Security Issues of Environmental Capture and Access

The security and privacy issues of context sensing are closely related to those of *capture and access systems*. Capture and access systems support the collection, storage, processing and distribution of information from environments of human action, specifically, multimedia information such as video and audio [169]. Capture and access software infrastructure (*e.g.*, the InCA system developed by Truong [168]) supports applications in domains such as the home [167], classrooms [168], and portable devices (*e.g.*, the PAL device described later in this thesis).

There is a conceptual affinity between context sensing and capture and access, because both collect and use information from the user's physical environment. However, the focus of capture and access systems is on collecting human experiences (audio/video depicting the users or their environment) for later use by humans [88]. Context sensing is somewhat more implicit and is often used by ubicomp applications to drive interaction or to mark up captured media.

Securing multimedia information captured from physical environments presents similar challenges as those described in the previous chapter with relation surveillance systems. One important difference is that in surveillance systems captured data is rarely used and stored past a certain retention time (*e.g.*, 30 days, depending on the local policy). Capture and access systems may be used for storing video and audio for much longer time and are designed with integrated information retrieval tools, explicitly facilitating access and further use of the captured material. Storage can introduce security liabilities. For example, the use of meeting capture systems in large commercial organizations may have been curtailed by concerns about the permanent storage and availability of recorded material to unauthorized parties [130].

Technical solutions for limiting access to information collected in capture and access applications include limiting access through control mechanisms that reflect the physical and social conditions in which the collection occurs (such as limiting access to the individuals who were present at its original capture) [98]. An alternative is that of deploying these applications in tightly controlled organizations or very public spaces where access control can be in part foregone (*e.g.*, classrooms).

Other solutions include the establishment of “physical privacy policy” spaces. Hewlett Packard has proposed, for example, a system that disables cameraphones in environments where a no-photography policy is posted, using short-range Bluetooth to signal the policy [146]. To avoid relying on the user terminal to comply with the policy, which raises issues related to technology control and trusted IT, Truong *et al.* have proposed a technique that prevents the use of cameras in certain environments, by beaming targeted light to the camera sensors, effectively blindfolding them [170]. In that paper, more techniques for preventing capturing images of physical spaces are cited.

3.2 Design Practice

It should be clear at this point that the security and privacy issues of collecting context and multimedia information about individuals are not limited to the technology (*e.g.*, the solutions for securing location information based on TTPs as opposed to anonymity systems). The larger social and economical environment directly affects the design and implementation of successful measures to ensure the security and privacy of ubicomp applications.

Along with technical solutions, several efforts have targeted the problem of developing *design methods* for identifying and solving security and privacy problems in general. These efforts recognize the difficulty of identifying and prioritizing issues and risks, and reflect the consciousness that technical solutions targeting individual security problems may not be sufficient without considering the broader social and technical environment of use. In citing related work, I will attempt to delineate the evolution of research on the design of ubicomp systems, specifically related to the development of design guidelines, design methods and analytic frameworks.

The proportionality method proposed in this thesis is positioned as a complementary contribution to other related efforts in the field of ubicomp security and privacy. In this thesis, when comparing other design approaches with the proportionality method, I suggest how my approach could be usefully employed within a larger integrated design practice, alongside, or instead of, other approaches. It should also be noted that the work cited below is limited to published, mostly academic, research and does not mention commercial systems which are often undocumented in the public domain.

3.2.1 Early Work: Privacy and Social Dynamics

As mentioned in Chapter 2, some early ubicomp applications were awareness and video media spaces (VMS) deployed in the context of workplaces, where social dynamics may resist the introduction of technologies resembling surveillance. Hence, analysis has extensively drawn from that of surveillance technologies, with a focus on privacy. On the contrary, security in ubiquitous computing has not been a topic of research early on.

3.2.2 From Awareness Applications to Evaluating Design Alternatives

Bellotti and Sellen published work on privacy in the context of VMS providing “awareness” and videoconferencing services. This work was in part based on the experience of the RAVE media space system at EuroPARC [72]. By using RAVE, remote coworkers could communicate directly even if not co-present, or simply “see” each order through the audio-video link, supposedly increasing opportunities for communication. Reflecting on this experience, Bellotti and Sellen developed a framework for addressing privacy issues in media spaces. According to their framework, the system should providing appropriate feedback and control structures to users [31]. Feedback and Control are described by Norman as basic structures in the use of artifacts [137], and are reflected also in the concepts of information and choice in the FIPS privacy principles. Bellotti and Sellen suggest devising appropriate mechanisms for feedback and control in four areas: capture, use, access and purpose for use.

Bellotti and Sellen also propose to evaluate alternative design options deriving from the analysis of feedback and control structures using a QOC (Questions, Options, Criteria) [123] evaluation process based on 8 questions and 11 criteria. Table 3.1 lists the questions on feedback and control proposed in this framework and the related evaluation criteria. Some of these criteria are similar to those employed in Heuristic Evaluation [136], a well-known discount usability technique for evaluating user interfaces. (Criteria that match Heuristic Evaluation criteria are marked with an asterisk *.) Among the criteria unique to Bellotti and Sellen's framework are those most closely related to security evaluation such as trustworthiness, and criteria that try to address the problem of security cost (ideally, security should come at no additional cost to the user): unobtrusiveness, low effort, low cost. 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.

Another early ubicomp system was an infrastructure used for locating people within an office complex called Active Badge and developed at Olivetti Research by Want *et al.* [176]. The system was installed in several research labs worldwide and was used for several purposes including call routing. In an evaluation of the system, Want *et al.* consider the privacy concerns ensuing from the system, including both general observations on privacy in workplaces and a discussion of the specific relationship between the developers and the system and the user base at Olivetti Research.

Table 3.1: Bellotti and Sellen’s Questions and Evaluation Criteria for VMS.

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 behaviours 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 behaviours 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 behaviours 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 behaviours.	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.

Evaluation criteria
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 behaviours 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.

Both the RAVE and Active Badge experiences exposed the delicate balance between privacy concerns and application usefulness. After the early work cited above, the interest in security and privacy in ubicomp generally subsided until the second half of the 1990's, when much of the security community's attention was drawn to other fields (the internet), and the ubicomp community was busy creating the first working implementations.

3.2.3 The Tradeoffs of Privacy, Control and Disruption

Recently, Lederer *et al.* have reiterated that successful designs must make information flows visible, provide coarse-grain control, enable social nuance, and emphasize action over configuration [120]. Fine-grained feedback about and control over information disclosure introduces an implicit design tension: more security implies increased administrative burden on the user who is called to oversee ever-increasing flows of information. This balance has been inquired specifically for context-aware technology by Barkhuus and Dey, who have suggested that people are willing to forgive some control over their personal location information to trusted individuals [25]. On the other hand, one of the conclusions of my own evaluation of a location-based application (the Reno application, discussed in Section 4.3.2) suggest that users do not desire automatic disclosure of location information—what Barkhuus and Dey term "active context-awareness"—in part due to potential sensing and interpretation errors that could mislead the recipient of the communication.

Privacy in media spaces is a recurring theme in ubicomp research. Hudson and Smith explored the privacy issues in awareness spaces [93] and proposed video manipulation techniques for reducing the invasion of one's personal space while providing others with cues about the activities that are happening there (*e.g.*, by using clever blurring algorithms). They point out that privacy cannot be considered in the abstract but is inevitably linked to other concerns including awareness and disturbance.

The tradeoffs between management and control are also discussed by Boyle and Greenberg in a comprehensive journal article that summarizes research on privacy in media spaces and attempts to provide a coherent framework to the problem [39]. They point out that in these applications, designers must consider:

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

Boyle and Greenberg thus introduce the factors of acceptance and perception management in the picture, pointing out that technical issues weigh heavily on potential deliberate privacy abuses, while human behavior and performance affects inadvertent privacy violations. They also propose to deconstruct the far-reaching concept of privacy into three aspects: solitude ("control over one's interpersonal interactions"), confidentiality ("control over other's access to information about oneself"), and autonomy ("control over the observable manifestations of the self").[23] After having described how these concepts can be used to analyze specific design questions in VMS, Boyle and Greenberg point out that there is still insufficient knowledge about the users to answer many of these decisions in a conclusive way. More than that, the authors point out the inadequacy of the analytic tools currently employed for mapping system functions with individual preferences and actions.

3.3 Turning to Experience and Practice in Related Fields

Given these pressing needs, recent work has continued generalizing the experience gained with the first working systems and has attempted to find solutions drawing from proven practice in related fields.

[23] Quotes from Boyle and Greenberg [39, p. 348].

3.3.1 The Fair Information Practices and Their Limitations

Langheinrich has proposed adapting the Fair Information Practices (FIPS) for driving the design of ubicomp applications [116].[24] The OECD's version of the FIPS is listed in Figure 3.1 [142]. Heeding this suggestion, Garfinkel has applied the FIPS to the analysis of RFID technology [69]. Patrick and Kenny report that a similar approach was used in the requirements analysis of an application developed by the EU PISA (Privacy Incorporated Software Agents) project [144]. Another way of using the FIPS would be as criteria in a QOC process framework (such as Bellotti and Sellen's).

While clearly still useful, today the FIPS are no longer sufficient for providing comprehensive design guidance. The FIPS reflect the top-down way in which system analysts designed potentially intrusive IT in the Seventies. Specifically, they only suggest evaluating if data collection is commensurate with the goal of the application. Using the FIPS requires the designer to have accepted a positive value judgment on the IT application at hand. It also requires the designer to have developed a thorough analysis and design of the data processing system. The FIPS do not address the fundamental concern of desirability of novel applications with open-ended technical designs—they just suggest how to approach the design once the application goals and their implementation have been selected.

[24] The FIPS were initially developed following work by Westin. They were adopted by the US Department of Health and Human Services as a basis for the 'fair' use of personal information [172]. They have constituted the base of data protection legislation across the world.

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 fulfilment 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 for purposes other than those specified in accordance with Paragraph 9 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 unauthorised 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.

Figure 3.1: The FIPS (OECD version).

Furthermore, the FIPS were thought specifically for the management of large databanks of personal information, such as health records, financial institutions or governmental records. Consequently, they may not be easily applicable in situations where 1) technology mediates relationships between individuals as opposed to between individual and organizations and 2) data is not structured and application purposes are ill-defined. Both are recurring characteristics of ubicomp applications. Consequently, the FIPS may fail the analyst in understanding whether an application is useful, acceptable to its stakeholders, and commensurate to its perceived or actual unwanted impact in the first place, especially when precedent lacks.

These principles provide guidelines to inform design but their generality and the lack of a design process model constrain their applicability. The proportionality method attempts to fill this gap by providing process guidance to reflect how people think about technology affecting everyday life. In some cases, the perceived usefulness of an application may convince people to adopt a technology that may be otherwise considered needlessly invasive, as reported, for example, by user studies by Barkhuus and Dey [25] and Melenhorst *et al.* [128].

3.3.2 Social/Technical Theories as Lenses for Interpreting Design Problems

The concept of feedback, highlighted by Bellotti and Sellen is also central to Palen and Dourish's description of interpersonal privacy as a continuous negotiation process [143]. Palen and Dourish apply to IT the theories on interpersonal privacy described by Altman [20] (in turn influenced by Goffman's work on individuals' behavior in social settings [77]). This work demonstrates that human and social factors may affect privacy as much as technology and that the boundary setting dynamics described by the social sciences can be applied to IT-mediated interpersonal relationships as well. One of the conclusions of their work is that applications must be carefully designed to enable such dynamics. Furthermore, they point out that individuals' expectations about the performance and retention of information in computer networks may not match reality.

3.3.3 Economic Frameworks May Be Difficult To Apply

A different approach is proposed by Jiang *et al.* in their Asymmetric Information Flows (AIF) framework. Drawing from economic theories and from an economic interpretation of personal information [155], Jiang *et al.* apply the Principle of Minimum Asymmetry to ubicomp design:

> *"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 flow of information from data collectors and users back to data owners." [110]*

The principle of minimum asymmetry should help reduce *externalities*, *i.e.*, the situation in which the parties benefiting from a transaction are not those carrying the associated risks. 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.

While eclectic and interesting in its theoretical approach, this model has a number of limitations. First, the authors have used AIF as an analytic tool, but to my knowledge, AIF has not been used to date as a design model. Moreover, potentially serious conflicts exist between this approach and data protection legislation in certain jurisdictions. For example, there are strong objections, both ethical and practical, to treating personal information (PI) as intellectual property. In some jurisdictions, privacy is considered an inalienable right and the sale of rights over PI is not foreseen. A practical problem with the idea of modulating confidence and accuracy of PI is that 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.

3.4 Elicitation and Design Techniques

The theme of design methods for tackling security and privacy in ubicomp subsided after the work of Bellotti and Sellen, mentioned above. However, recently, several researchers have attempted to further the state of the art in this domain by proposing alternative design techniques. These attempts are in part a response to the complexities of the design space, and reflect a need for reducing the cost of analysis and design, which in QOC processes can be relatively high.

3.4.1 Reducing Costs Using Patterns

Chung *et al.* have applied the concept of design patterns to privacy problems in ubicomp [45]. The privacy patterns used in that study are listed in Table 3.2. Chung *et al.* evaluated their method using a design exercise in which both students and experienced designers used the patterns to perform an assigned design task. The authors point out that the privacy design patterns were not used in any meaningful way by the test designers; also, expert reviewers did not evaluate the designs produced by those using the patterns to be better than those produced by designers in a control condition.

Table 3.2: Chung *et al.*'s Privacy Patterns.

Pattern	**Description [46].**
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 his or 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.

My experience suggests that, while patterns are helpful in established areas [19], it may be premature to apply them in the ubicomp domain (Chung *et al.* acknowledged this mismatch by terming their patterns “pre-patterns.”) In situations of exploratory design practice, only thorough analysis on a case-by-case basis can provide strong arguments for an application’s acceptability. As suggested below, the proportionality design process attempts to be more flexible by describing design features as elements that can be composed with one another.

3.4.2 Striving for Completeness: Goal-Driven Analysis

A recent design method developed at our institution by Jensen *et al.* is STRAP (Structured Analysis Framework for Privacy). STRAP can be used to derive privacy vulnerabilities from a goal-oriented, iterative analysis process, and is composed of three successive steps: vulnerability analysis, design refinement and evaluation [108]. Although it is not tailored specifically to ubicomp applications, STRAP may be used to identify vulnerabilities and inform design decisions. Initial analysis of STRAP’s performance, through design exercises, suggests that designers using STRAP identified more privacy issues, and more quickly than a control group (which used a variation of Bellotti and Sellen’s framework). The evaluation of the STRAP method and of the design patterns by Chung *et al.* is interesting in the context of this thesis because I adopted a similar evaluation technique for the proportionality method.

3.4.3 The Tension between Quantitative and Qualitative Risk Analysis

Hong *et al.* propose a risk analysis approach for studying privacy in ubicomp applications [92]. Their process enhances standard risk analysis by providing sets of social and technical questions to drive the analysis, and heuristics to drive risk management, all tailored for ubicomp applications. The questions Hong *et al.* propose are listed in Table 3.3. The authors propose a semi-quantitative risk evaluation framework, suggesting to act upon each identified risk if the standard “C < LD” equation is satisfied.[25] To evaluate the variables in this formula, the authors propose a set of risk management questions, listed in Table 3.4. The authors point out that quantitative evaluations are difficult to make in most cases and should in any case only be used for prioritizing risks and corrective action. In particular, it is difficult to estimate the economic impact of unwanted disclosures of personal information especially when they occur in interpersonal settings. In addition, critics of quantitative approaches also point out that quantitative assessments may prove misleading, failing to consider user perceptions and opinions. The risk analysis framework, though originating from the authors’ extensive experience in the field of ubicomp design, has not been evaluated to verify its effectiveness.[26]

One substantial problem lies in identifying risks correctly and exhaustively—which calls for investigating users’ opinions and perceptions. Chapter 6 provides an extended discussion on the problems of user inquiry in ubicomp. Although risk analysis is a fundamental component of security engineering, many aspects of design in this domain cannot be framed in a quantitative manner, and a qualitative approach may be necessary. An interesting qualitative approach to risk analysis for ubicomp is provided by Hilty *et al.*, who suggest using a risk analysis process based on risk screening and risk filtering [90]. In the screening phase, an expert panel identifies relevant risks for a given application (thus using the expert’s experience directly, instead of the social and technical questions suggested by Hong).

[25] 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.

[26] J. Hong, personal communication, July 12, 2005.

Table 3.3: Hong et al.’s Risk Analysis Questions.

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 3.4: Hong et al.'s Risk Management Questions.

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?

Then, risks are filtered according to qualitative risk prioritization based on the following criteria, derived from work in the German risk assessment community:

- 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 use this framework for analyzing a number of risks of ubicomp technologies, including risks deriving from wireless communications' radiations, the social effects of the technology and its environmental impact. However, while their heuristics are adequate for analyzing macro-social risks, they may not be adequate for risks arising at the interpersonal level.

3.4.4 Multilateral Security and the Problem of Brokering Competing Needs

The concept of *multilateral security* has influenced much of my research in security and privacy over the past several years. Multilateral security was developed for analyzing systems with multiple competing security threats. The theoretical background and methodological approach of multilateral security stems from research done in the German e-commerce and data protection communities during the 1990's [132, 153].

One of the innovations of multilateral security is that it frames privacy requirements and solutions as security requirements. According to multilateral security, security and privacy are different expressions of the same balancing process among contrasting interests within a system or application. The purpose of this balancing is that of achieving technological solutions that are acceptable to users, while being at the same time 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, it highlights the role of designers in producing equitable technology, and that of users who are to be empowered to set their own security or privacy goals.

The multilateral security framework was applied to several case studies, including a prototype mobile application for mobile "reachability" management (*i.e.*, brokering availability to incoming phone calls). In that case study, Rannenberg documented how user studies can help design mobile applications with multilateral security requirements in workplaces [152].

The determination of a compromise between competing needs in the design space is one of the cornerstones of the design method I propose. Requirements compromise is a long-standing issue in software engineering research and several techniques have been used for making such determinations. For example, Boehm *et al.* describe the WinWin requirements negotiation model [36]. That model's purpose is to broker among requirements that are competing because of cost constraints and is thus eminently quantitative. In our design space, it may not be possible to negotiate requirements in a purely quantitative manner, due to the impossibility of associating a value function to the design options and consequences on stakeholders. However, the spirit of this balancing process is somewhat similar to our case. Prioritization techniques used in qualitative risk analysis and mentioned above may aid the designer in selecting which competing requirements must overrule others, especially if individual requirements cannot coexist in a design solution.

However, even risk analysis may be an inadequate tool for deciding between competing requirements, because design decisions may 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 [93] and Barkhuus and Dey [25] mentioned above.

3.5 Rationale as an Answer to Uncertainty in Design

The design method proposed in this thesis advocates careful evaluation of the design space and the reasoned justification of competing design choices. Reasoned documentation of design choices is one way in which the design and software engineering communities have approached hard, undefined problems in the past. For example, in Design Rationale work of the late 1980's, MacLean *et al.* suggest that documentation of design choices (through a QOC process) does not only provide record of the design decisions taken but is integral part of the design process itself and can improve the quality of such process [124]. MacLean *et al.*'s interest was in the development of user interfaces, but they acknowledged that Design Rationale could be used for other domains as well.

Approximately at the same time of the Design Rationale work, the security community was also grappling with similar design documentation issues. The complex requirements space of security-critical IT products requires rigorous justification and the traceability of design choices for evaluation purposes. The Common Criteria for IT Security Evaluation and Certification, developed starting in the early 1990's to facilitate the evaluation of security in IT products, mandate the use of Protection Profiles for achieving this goal [105]. Protection Profiles are documents that trace functional security requirements back to security objectives, and these in turn to security threats. At each step, the author of the Protection Profile uses design rationales to prove the relations between threats, objectives and requirements. These rationales must be argued more or less tightly, based on a claimed Evaluation Assurance Level (increasingly high Assurance Levels require progressively stronger rationales, from informal justifications up to mathematical modeling and proofs).

The market success of the Common Criteria has been arguably limited by the high costs associated with their use. Moreover, while Protection Profiles must include a thorough rationale to guarantee that system analysts have exhausted the design space, the requirements set proposed by the standard is fixed. A fixed set of requirements makes the standard apt for well-understood applications for which a "best practice" design solution is available, and to traditional systems that do not present competing security requirements. By contrast, the unique problems of the ubicomp domain demand more flexible solutions, which can broker competing requirements in atypical applications.

3.5.1 Prescriptive vs. Generative Design Methods

Above, we compared the merits of the different design techniques, namely design patterns, AIF, FIPS-based design guidelines, QOC analysis, and Design Rationale. It emerges from this discussion that prescriptive approaches to solving ubicomp security and privacy problems may not provide sufficient guidance to designers. This is a recurring theme in this thesis and will be further discussed in Chapter 6.

First, the design space is too large and ill-defined to support prescriptive approaches such as patterns, which base their validity in deep, long-standing design practice (*e.g.*, Alexander's *The Timeless Way of Building*). The observations documented by Chung *et al.* with the use of privacy patterns to design ubicomp applications supports this claim [45].

Prescriptive guidelines based on the FIPS, such as those proposed by Langheinrich [116], may also fail to provide detailed design guidance. For example, several researchers have pointed out that in interpersonal relations, the identity of the individual receiving personal information is a primary factor influencing the disclosure preferences and behaviors (*e.g.*, work on location disclosure by Consolvo *et al.* [51] and on multimedia communications by Adams and Sasse [18]). This factor is not taken into account by the FIPS. As yet another example, design guidelines such as “Access and Recourse,” while applicable to the relationship between individuals and organizations, may be difficult to apply to interpersonal communication.

If we accept these observations, it follows that it might be more effective to search for solutions in non-prescriptive or *generative* design methods, such as those embodied in QOC or Design Rationale and risk analysis. By generative, I mean design methods that help generate the relevant design questions, rather than provide guidance on solutions. Plain QOC leaves the designer, however, with the problem of asking the right questions. Likewise, risk analysis presents the problem of identifying the relevant risks. Once questions are asked and risks are identified, it is necessary to prioritize the risks and reach reasoned answers to the design questions. All this requires designers to go to the source and study the intended users of the systems under consideration. The last part of this chapter will investigate this problem, which turns out to be much more subtle than just applying established user-centered design (UCD) practice.

3.5.2 Understanding Stakeholders' Concerns

Analyzing privacy and security issues in ubicomp applications presents numerous challenges to effective user-centered design (UCD). Some of these challenges are general and derive from the nature of ubicomp systems. Understanding usage environments requires designers to step out of the lab and follow people where they use these applications—on streets, in shopping malls, homes and wherever else they might go. Furthermore, evaluation must also occur in a "situated" setting in order to account for physical and social interaction, disruptions, variations in cognitive load, and other environmental factors that can profoundly impact the usability and usefulness of mobile applications [14].

Probing users' opinions and preferences about IT security also represents a hard problem. Identifying security requirements has been a traditionally difficult problem that has prompted the development of security standards such as the Trusted Computing Security Evaluation Criteria [53] and, later, the Common Criteria. In most cases, security requirements are non-functional and most people may have difficulty expressing their needs and concerns in a way that can be fed into a requirements engineering process. Security requirements elicitation represents a research field in itself.[27]

Multilateral security suggests that when seen from the user's perspective, many privacy requirements can be reinterpreted as user-centered security requirements. However, probing privacy introduces further challenges. For example, people often take a deontological stance when artificially probed on opinions and preferences on privacy, both in reference to organizations [33] and in interpersonal relations. Everyday behavior may differ from stated preferences for many reasons, including insufficient informational

[27] For example, a Software Engineering for Secure Systems workshop was recently held in conjunction with a major Software Engineering conference.

awareness (ignoring the fate of collected information), overriding primary goals (getting a transaction done), or carelessness (not wanting to bother with evaluating every exchange of information), as pointed out by Acquisti and Großklags [16]. On the other hand, people have a very refined sense of privacy balance in interpersonal relations, as described by Altman [20], and may choose certain paths of behavior to avoid conflict or in response to overriding social goals.

It follows that abstract or purely self-reflective surveys may be insufficient for probing privacy concerns. This observation applies in general to all those situations in which people may be unable or unwilling to verbalize their behavior abstractly, from complex social constructions, as pointed out by Goffman [78], to the formulation of procedural plans as noted by Suchman [161]. In addition, people may be unable to grasp immediately the effects on their socio-technical practices of new technologies being introduced in familiar settings.

In the past few years, several researchers have attempted to study users' needs and concerns in the domain of privacy and security in ubicomp. Particularly interesting projects include Beckwith and Lederer's interviews with elder-care residents and caregivers [29], Consolvo *et al.*'s experience sampling surveys to probe privacy requirements in a situated setting [51], Barkhuus and Dey's work on location technologies on a US university campus [25] and Kindberg's work on trust in *m-commerce* payment systems [111]. Moreover, work in the HCI community has started to focus on in-the-field prototyping to address the challenges related to testing and evaluating ubicomp applications: the concept of Experience Prototypes described by Buchenau and Suri [41] and the use of Wizard-of-Oz techniques in mobile settings [58, 122] are aimed at evaluating mobile technologies within iterative development processes. However, more work is needed to develop reliable and efficient UCD tools for gathering security and privacy requirements for ubicomp applications.

3.6 Beyond Design Techniques

In this chapter, I have argued that the most effective design techniques for tackling security and privacy problems in ubicomp may be case-by-case, labor-intensive methods based on the evaluation of alternative design options and risk analysis. Prescriptive design tools, such as design patterns have not been very successful. Also, general design guidelines have proven of difficult application and of uncertain effect. This suggests that the field is still in its early stages and it may be premature to propose 'shortcuts' or simplified guidelines or patterns for addressing these problems. These approaches may be more appropriate for disciplines with an established practice. Generative design and risk analysis are appropriate instruments for not-well known fields. In particular, Bellotti and Sellen's approach uses design questions to address security and privacy issues. Hong *et al.* have attempted to facilitate risk analysis by providing a set of questions relevant to the ubicomp domain that can be used to identify risks. An integrated approach should include an end-to-end way of thinking about the problem, including appropriate requirements analysis and design tools. Such an integrated approach will be presented and evaluated in the following chapters.

CHAPTER 4

THE PROPORTIONALITY DESIGN METHOD

In Chapters 2 and 3, I argue that attempts to manage the privacy and security implications of ubicomp technology have not been very successful. Although there have been numerous proposals to model security and privacy concepts, principles and requirements, there is still a lack of understanding of specific applications and contexts. For example, the Asymmetric Information Flows framework proposed by Jiang *et al.* proposes to reduce the asymmetry in knowledge between individuals by modulating three properties of information—persistency, accuracy and confidence [110]. Ignoring the technological and legal obstacles mentioned in Chapter 3, the AIF framework suggests a way of achieving certain privacy goals, but does not help in understanding *what* these goals are. Nor do design principles, such as Information Minimization[28] help to define these goals. As pointed out in Chapter 3, by the time the designer can apply these principles, he or she has already accepted a positive value judgment on the IT application at hand. My conclusion is that there is a need, within the community of researchers and developers of ubiquitous computing technologies, to step back and reconsider what we want to achieve with each of these technologies.

When using these privacy frameworks and design principles, the designer still faces the challenge of deciding whether the application is desirable and acceptable for the

[28] Information Minimization: a principle derived from military need-to-know policies and used in the privacy community whereby the collection of personal information is strictly limited to the minimal amount sufficient for enabling the delivery of the related services. Information Minimization is not included in the FIPS. OECD's version of the FIPS only call for a weaker 'limitation' of collection and use [142].

intended market. It should be noted that this is hardly a novel problem in IT development. Over the years, the scope of IT development has expanded repeatedly to encompass organizations, users, their concerns and motivations, for example in terms of User-Centered Design (UCD) in the 1980's [139], or, more recently, with Value-Sensitive Design [68]. Therefore, I view this work as providing some suggestions on how to approach security and privacy issues, in the long-standing tradition of UCD. The novelty of my work consists in the specific application of UCD to problems in the ubicomp domain that have been approached traditionally as merely technical issues.

In light of the discussion in Chapter 3, a user-centered approach to security and privacy issues in ubicomp must consider both the macroscopic and microscopic levels. At the macroscopic level, a general approach is needed for tackling security and privacy issues in ubicomp. At the microscopic level, it is necessary to gain a better understanding of users' concerns and needs in relation to specific applications.

As a final remark, I would like to point out that I am intentionally avoiding an ethical discussion on privacy and security. While I acknowledge the importance of adopting an active stance towards privacy protection and increasing information security, I also believe that many other authors have stated the ethical, as well as economic and social case for developing IT that is both more privacy-sensitive and secure and that there is no need for replicating such discussion (*e.g.*, Lessig [121], Etzioni [60], and governmental reports [148]).

An initial step in accomplishing the first part of the research program outlined in the Introduction is represented by my proposal of the proportionality design method [97], presented in the remainder of this Chapter. In Chapter 5, I describe an initial validation of the design method in two design experiments. The second part of the research program, documenting UCD techniques for probing privacy and security concerns in ubicomp applications, constitutes the main topic of Chapter 6.

4.1 The Principle of Proportionality

A vast body of knowledge regarding the impact of technology on privacy has grown over the past century in rulings and opinions issued by courts and, more recently, Data Protection Authorities (DPA)—supervisory entities with regulatory and enforcement powers on data protection matters. Among the tools developed by these communities to tackle socio-technological problems, the *principle of proportionality* has been used repeatedly in reference to privacy and security. In this thesis, I develop the idea of proportionality into a design method that can provide guidelines for the design of secure and privacy-preserving ubicomp applications. In this context, I define the principle of proportionality as follows:

> *Any application, system or process should balance application goals with the privacy and security concerns of all involved stakeholders.*

The above definition is rather general and DPAs have typically interpreted proportionality in a rather narrower fashion, as a balance of *application usefulness* with *privacy rights*. For the purpose of this work, I would like to maintain a more vague definition of the principle, leaving specific details to the method description given below.

This very general principle may resemble one of the Fair Information Practices, namely Data Quality.[29] As noted above, however, proportionality differs in one important aspect from Data Quality, because it establishes a balance between the *goals* of the considered application and its effects on privacy, whereas the FIPS only impose conditions on the collection and use of information in relation to the data subject's consent, and to the needs of the application. In this sense, the FIPS reflect how system analysts designed

[29] 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." [142, §8]

potentially intrusive IT in the Seventies, while proportionality reflects how people might think about technology affecting everyday life (*e.g.*, Barkhuus and Dey report that users of location systems are willing to forgo a degree of control on their location information if this enables useful services [25]; Melenhorst *et al.* report that the invasiveness of home monitoring systems for the elderly may be acceptable in the face of an increased perception of security [128]).

Recent data protection regulation has specific provisions for proportionality between utility of data collection and its burden on data subject's privacy. European Union Directive 95/46/EC (the baseline for all EU Members' data protection laws) states that "personal data may be processed only if … processing is necessary for the purposes of the *legitimate* interests pursued by the controller or by the third party or parties to whom the data are disclosed" [1, §7(f), italics by the author]. In this case, assessing legitimacy requires a balance between benefit of data collection and the interest of the *data subject* (the person to whom the data refers) in controlling the collection and disclosure of personal information. European DPAs have expanded and clarified the proportionality principle by providing opinions on applications of automated sensing technology mentioned in Chapter 2 [61, 62].

This balancing of interests is, of course, not unique to the European data protection community. For example, opinions involving the "chilling" effects on First Amendment rights of surveillance in public space in the US (*e.g.*, during public demonstrations) [30, p. 168] point out a balancing between the interest of preventing crime and individuals' rights to free expression. The *Bartnicki v. Vopper* case of 2001, cited in Chapter 2, shows that arguments on the impact of technology on privacy are based on balancing of privacy rights with the public's right to know. Furthermore, the concept of reasonable expectation of privacy (*Katz v. United States*, 1967 [5]) implies a proportionality judgment on the perceptual qualities of sensing technologies.

It is safe to say that the principle of proportionality is widely used across legal contexts to balance technology and privacy.[30] However, court rulings and DPA opinions are extremely general and do not provide operative guidance to designers, because they emphasize summative and technology-neutral critique. The contribution of this work consists of a structured, flexible design method for ubicomp applications, inspired by legal and technology policy evaluation and based on the experience gathered developing and evaluating ubicomp applications, and observing other deployments. The design method is intended to be helpful to IT developers and researchers. In particular, the objective of the design method is to:

- structure the design of ubiquitous computing applications based on the evaluation of their impact on stakeholders' privacy and their usefulness;
- compare alternative designs (user interface options and information policies) within the design space to maximize adherence to stakeholders' requirements (by compromising among competing requirements if necessary).

Two observations are necessary at this point. First, I recognize that it may be impossible to achieve unanimity among the users and designers of any one application. The purpose of this design method is not that of achieving 'objective,' unanimous results, because many of the decisions involved in the application of the method are inherently subjective and based on heuristic value judgments. I do not seek utopian agreement by all users and designers involved in ubicomp applications with security and privacy implications; more realistically, I strive to ground design on convincing and comprehensive reasoning based on user and social understanding, legal precedents, and industry best practice. The proportionality method invites designers to approach design with a critical eye

[30] This analysis is limited to EU and US laws because the abundant and easily accessible literature and reflective stance adopted in these jurisdictions provide useful insight. Privacy laws in many other parts of the world resemble either model.

open to alternative solutions, in the conviction that a rigorous stance to privacy does not curb development, but increases the chances of acceptance and of success.

Second, the ‘balancing’ of privacy and usefulness does not necessarily imply a quantitative assessment. The social practices and design requirements associated with privacy and IT security are much more complex and nuanced than a reductive quantitative approach would assume. While certain design parameters may be quantified and manipulated to meet user requirements (*e.g.*, retention time), this is not true in general. In fact, my experience shows that, in many cases, quantitative tradeoffs are not appropriate to represent or model user needs. The balancing should be viewed instead in a more general manner, as trying to achieve a coherent and successful design in situations where there might be contrasting needs and concerns between multiple stakeholders and or even just one stakeholder.

4.2 From Principle to Design Method

The definition of the proportionality principle provided above is simple, but it does not translate well into a process for building applications. Design is about making decisions, progressing from a problem statement to a solution. In attempting to cast the principle of proportionality within a design framework, therefore, it is necessary to account for that decision process. My method begins with the driving motivation from the principle of proportionality, the establishment of a design balance among competing needs, and proceeds toward a systematic refinement to whittle down design alternatives in the face of security and privacy considerations.

Before applying the method, the designer must identify the relevant stakeholders, and select a small number of application goals that form the characteristic kernel of the application. There are many ways to express these goals, including stating abstract requirements, describing usage scenarios, or providing a high-level description of a system. Specifying the application goals very precisely may result in more accurate conclusions, but the design space may be constrained needlessly. In the two case studies reported in this Chapter (the Personal Audio Loop and Reno), application goals are stated through a high-level design description, because I entered the process at a stage in which an initial design had already been developed.

The design method is divided in three stages (see Figure 4.1) [97]:

- Desirability—Establish that the application goals would meet the needs for the intended user population.[31]
- Appropriateness—Recommend the best technological (or non-technological) implementation solution.
- Adequacy—Within a given technology, identify the parameters that can be adjusted, and examine them to justify proper use.

In very blunt terms, *desirability* and *appropriateness* are typical of the structure of the analyses performed by DPAs and courts, while *adequacy* refers to the fine-grained activity of interface and system designers. Desirability and appropriateness, as defined above, are questions of social relevance often overlooked by designers and researchers who may be driven by the immediate benefits of novel applications.

The design method is simple, in order to be integrated within a traditional UCD development process. In fact, the intention is that the proportionality method should be used to generate relevant questions that must be answered within UCD by using appropriate tools and techniques. The iterative nature of the design method is shown Figure 4.1, reflecting what is commonly considered the best practice development model by the UCD community.

[31] In previous publications, this step was named *legitimacy*. It was renamed *desirability* to avoid implying a direct reference to legislation and a mechanical and “economic” view of the process of balancing stakeholder needs.

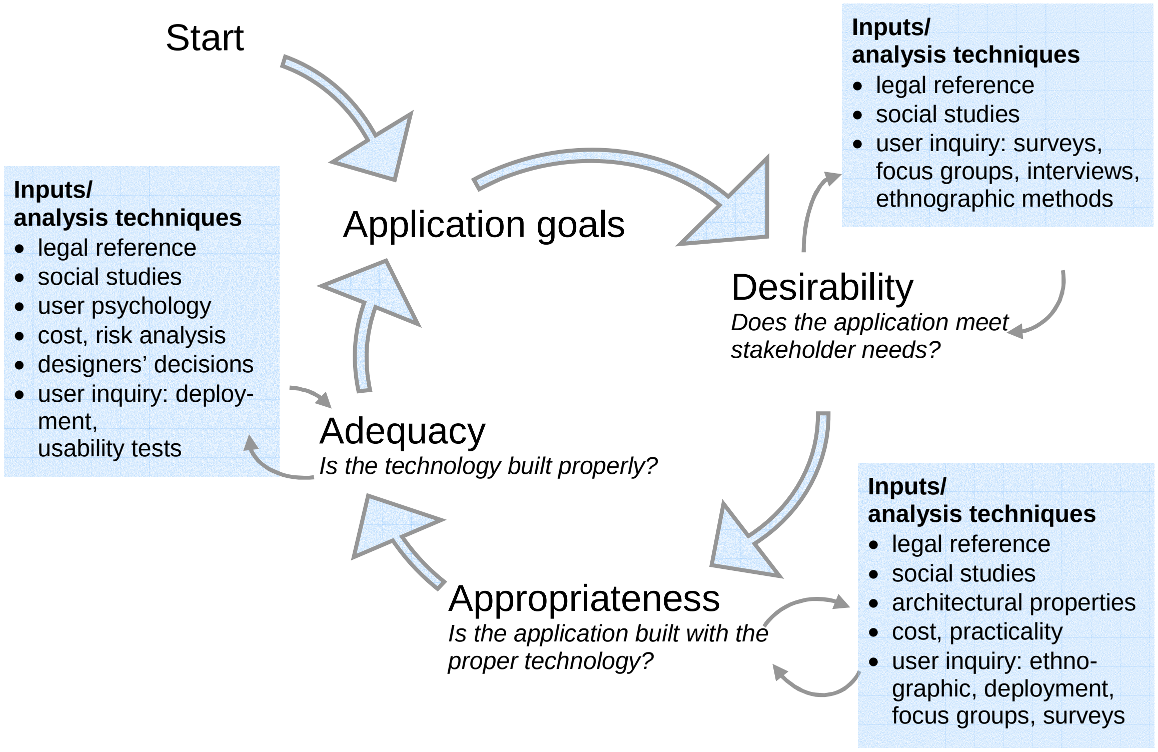


Figure 4.1: The proportionality design method at a glance.

The process starts with the definition of application goals and continues through successive refinement of design issues and solutions. The boxes list analysis techniques that I have found useful at each stage of the analysis process for generating and verifying requirements and design constraints.

Such an iterative depiction does not imply, however, a commitment to one specific development model (*e.g.*, spiral *vs.* waterfall), nor a 'continual improvement' approach to design. Designers should tailor the length and number of iterations to the specific development environment and application at hand.

Below, I provide a short description of each stage. This discussion is not intended to be exhaustive. Rather, my goal is to suggest how the three stages can be approached and to note which sources and techniques I found useful in making design decisions at each stage. I have applied the proportionality method to an application developed within our research group (the Personal Audio Loop, a mobile short-term audio memory aid tool) [87] and to Reno, a mobile application used to disclose the user's location, developed at Intel Research [158].

4.2.1 Desirability

The first step in the proportionality method requires the designer to assess whether the potentially conflicting needs of the stakeholders are met. For a given application (*e.g.*, a home security system), one must demonstrate that the interest in using it *for a specific purpose* is compatible with stakeholders' concerns (*e.g.*, about their personal privacy or security) and other externalities (*e.g.*, the concerns of unrelated passersby, visitors). In many cases, DPAs and courts address the issue by structuring the problem along the following three questions:

– What is the purpose of the application?

– What are the advantages gained? (*e.g.*, expressed in reduction of risk, or economic benefit.)

– What is the imposed security or privacy risk? (*e.g.*, in terms of changes of behavior, "chill effect," or other social costs.)

Answering these questions requires the designer to engage in a documented and justifiable design process. The *purpose of use* of an application is closely related to its intended benefits, and thus is integral to the desirability assessment. For example, the

French DPA allowed a video surveillance system with license plate recognition at border crossings to increase customs control accuracy and throughput. In contrast, the DPA did not allow a very similar system, intended for increasing quality of service on motorways, because the benefits (improved congestion management) were not deemed to outweigh the potential effects of large-scale tracking of private vehicles on internal motorways [40].

Identifying the *advantages gained* might be as simple as reviewing the application motivation, although emergent use adds uncertainty to such determination. Identifying *imposed burden* may be more difficult. A multilateral security threat analysis can yield comprehensive answers, although characterizing threats might prove difficult. Although risk analysis may be used to identify threats (Hong *et al.* specifically proposed using risk analysis for ubicomp privacy [92]), more qualitative arguments are often the only viable option. Various methods can be employed for gathering qualitative evidence, including standard legal priority determinations (*e.g.*, economic advantage is subordinate to freedom of speech), judgments made by courts on similar applications, and industry best practices and guidelines.

Defining stakeholders' needs in terms of benefit and burden (and the design process as a balancing act) does constrain the breadth and depth of the analysis and design spaces because it projects all design variables on a one-dimensional scale.[32] As mentioned above, this formulation is typical of courts and DPAs, and is particularly fit for applications, such as surveillance, which can hardly be maneuvered, after deployment, by concerned individuals to achieve social goals. However, the case studies below demonstrate that the balancing process is not necessarily one-dimensional, but involves several competing stakeholders at the same time. In fact, many ubicomp applications demand a

[32] P. Dourish, personal conversation, April 2005.

more flexible design approach, capable of dealing with, for example, the boundary setting process involved in the management of personal privacy (or, in multilateral security terms, “empowering” users) and in the management of the practical security features of the application. This increased flexibility is also needed to support the view of ubicomp as a set of *environments* with potentially multiple uses, rather than as a collection of discrete single-purpose applications.

4.2.2 Appropriateness

Once the need or desirability of a certain application has been established, the appropriateness of the alternative implementing technologies or techniques must be evaluated. Cost and practicality are obviously important co-determinants in this assessment. Moreover, it may not be possible to select a technology for a certain application disjoint from individual needs (that is, appropriateness and desirability may be indivisible), especially in cases where design is driven by technology as opposed to by users’ needs.

Therefore, the distinction of these two phases should not be considered dogmatically, but rather as an artifact useful for certain kinds of applications, in which goals and technology can be analyzed separately. In brief, the main questions of an appropriateness determination are:

- Do the cost and quality of the selected technology justify the potential invasion of privacy with respect to alternative solutions?
- Does the technology pose the risk of being abused or employed with further security or privacy implications?
- Can the application goals be reached by other means (including non-technical)?

Note that there is a similarity between these questions and the SE concept of *validation*. Although different technologies can be used to attain an application goal, not all technologies have the same effects on privacy. As a practical example of this, consider security systems: audio recording is in many cases considered more invasive than photographs. This thinking is mirrored by a 2002 opinion given by the Swedish DPA that disallowed an in-vehicle security system in taxis employing audio recording, whereas it permitted digital pictures of passengers to be taken at the moments when they entered and left the car [40].

Technological choices are influenced not only by the technical merits but also by their wider social ramifications. For example, in an ethnographic study of video surveillance operators, members of ethnic minorities and conspicuously dressed people were more often targets of surveillance than ordinary looking people [140]. Furthermore, designers often overlook non-technical solutions for meeting a certain goal. For example, research conducted in the 1980's and 1990's on graffiti and vandalism prevention strategies showed that the installation of surveillance cameras is not necessarily the only or best solution: cleaning graffiti promptly or enacting prevention programs instead provides equally good results [73].

The selection of the appropriate technology might contrast with the designer's preference in terms of implementation cost, and might also reduce flexibility for future development. Moreover, emergent uses may unsettle a delicate design balance. In this perspective, the desirability and appropriateness determinations should not be viewed just as a mechanical selection of a technology that reaches specific goals. Rather, the process is also meant to result in the definition of management, deployment, and usage conditions, of corrective or balancing measures, and in the revision of the application goals in order to curb undesired effects.

4.2.3 Adequacy

As the design process deals with increasingly fine-grained aspects of the application, the third stage of the design process examines the qualities of the chosen application and technology, which must be adequate to the application goals and acceptable to all stakeholders. This stage bears resemblance to the SE practice of *verification*.

Arguing the adequacy of specific design choices can become very laborious, because the design space can expand to include many interdependent features, such as user interface affordances, information policies and internal parameters. Further, while traditional IT security and privacy benefits from a long experience of regulation and industry best practice, the ubicomp design space has many more "degrees of freedom." In addition to retention time and disclosure policies typically used in traditional data protection, the ubicomp design must also account for proxemics, architectonic features (enclosure, delimitation, *etc.*), and social variables (*e.g.*, artifact ownership, whether it is a public space or not).

Interface and cognitive affordances, sensing modes and management policies are fundamental for the adequacy test. For example, the Article 29 Working Party (the European advisory body on data protection) discusses the case of a doorbell camera, used to identify visitors standing at the door. Here, the fundamental features are the shot angle and cone and activation mode of the camera [61]. A narrow-angle lens, pointed at space outside the path of unrelated passersby, and activated by the visitor pressing the doorbell, is acceptable in most social settings. Indeed such installations are deemed legitimate and appropriate. Conversely, a remotely controlled system, capturing an ample portion of the street or corridor, does not provide a satisfactory compromise of benefit and burden, because it collects much unnecessary information.

The analytic technique to use for this assessment depends on the technology as well as the deployment setting. I present here a very simple procedure, inspired by multilateral security and WinWin requirements engineering models [36], which is based on the five steps of Figure 4.2.[33] This method was used in the two case studies below. Prelimi-

[33] I do not claim that this is the only or best way of performing this analysis. In fact, this analysis has several drawbacks (for example, it ignores temporal and cultural variables).

1. *What are the characteristics of the privacy- or security-impacting design features? E.g.*, impacted spatial area (*e.g.*, microphone range or lens angle), measurement resolution, level of aggregation of data, aspects of the user interface (data access interfaces and operation mode).
2. *How are design features described as variables?* By type (*e.g.*, discrete or continuous) and range (*e.g.*, minimum and maximum, selection of choices), considering the characteristics of the employed technology.
3. *What are the values or ranges of each variable critical to the success of the application? E.g.*, the accuracy of a location technology.
4. *What are the values or ranges of each variable which impact on the privacy and security of all stakeholders?*
5. *What compromise is possible between the requirements of steps 3 and 4, considering their relative validity?*

Figure 4.2: Simple Adequacy Process.

nary experience in its application within the development process suggests that it improved understanding of the associated uses and risks, and of the corrective actions necessary within the deployment environment. More work would be necessary to verify this procedure's effectiveness with other types of ubicomp applications.

The characteristics identified in step 1 in Figure 4.2 include a very wide assortment of design features. Privacy principles such as the FIPS can be used to generate guidelines and identify relevant design features specific to the application at hand. Here I list five types of features that have been particularly relevant in my experience:

- **Quantitative measures of sensor precision**. In the case of location sensing, for example, lower resolution is associated with greater uncertainty, which increases plausible deniability, and thus indirectly, user privacy.
- **Quantitative measures of sensor reach**. For example, the range of a microphone can be modulated responding to information minimization principles.
- **Interface affordances for data retrieval**. Access cost to collected information (*e.g.*, required time, whether access attempts are made public) can

be considered in an adequacy assessment. As access cost increases, the number of accesses decreases, increasing privacy.

- **Technology visibility**. Understandable cues of personal data collection increase privacy by enabling knowledge (thus supporting informed consent dynamics and self-restraint).
- **Preexisting understanding of the used technology and metaphors**. Cultural baggage can reinforce or interfere with the understanding of technology's properties and operation.

In step 2, the identified characteristics must be described by indicating their variability range, and whether there are relationships amongst them (*e.g.*, design tradeoffs, cost tradeoffs, or external bounds). Clearly, design characteristics are not always amenable to such a reduction; although a quantitative description of design features simplifies the subsequent proportionality arguments, the designer must be prepared to consider more complex, or non-quantifiable, characteristics. It should however at least be possible to determine the bounds of the design space.

In step 3, the designer must select which characteristics and values are critical to the success of the application: what characteristics are hard as opposed to soft requirements. Similarly in step 4, the relationship between design characteristics, their values and the privacy burden to all involved stakeholders is evaluated. These determinations can be reached through a vast mix of design tools, provided that an adequate rationale is provided. The confidence that these tools provide is key to the adequacy process at this stage. Deployment, usability studies, interviews and analytic tools provide the firmest grounds to determine appropriate ranges for design variables. However, any design process is permeated by countless decisions made by the designer which cannot all be conclusively accounted for. What the proportionality method calls for is that these judgments be made explicit and used as afforded by the value of and confidence in the supporting evidence.

Finally, in step 5, these assessments are compared, and individual proportionality judgments are made for each variable. The determination of a compromise in the design space constitutes the kernel of the design method. Various techniques can be used for making such determinations, *e.g.*, requirements negotiation models such as WinWin [36]. For simplicity, I do not discuss how to manage mutual effects between individual adequacy judgments. There are several possible options in case the ranges identified in steps 3 and 4 clash.

- It might be necessary to decrease the success requirements of step 3.
- The designer might reconsider privacy goals identified in step 4 (by yielding to the other party's interests).
- It might be possible to reconsider any specific application goal that is bound to requirements that cannot be satisfied (in extreme cases, the designer might resort to abandoning the specific application altogether).
- The designer may choose a different technology for meeting the same application goals.

The case studies below illustrate both cases in which requirement negotiation was straightforward, and cases in which reaching a compromise required to modify success or privacy requirements.

4.3 Examples of Applying the Proportionality Method

The aim of this work is that of developing design guidance for the development of ubicomp systems and applications. To achieve this goal, reference to working applications is essential. Over the course of the past two years, I studied several ubicomp systems, both developed at this Institute and externally. These systems include the Personal Audio Loop, a personal, portable, audio memory aid device [87] and Reno, a peer-to-peer mobile, location enhanced messaging application [51, 99, 158].

These case studies were selected for several reasons. Both applications are likely to expose security, privacy and control issues of interest because they are based on the collection and use of personal information. In both cases, the collection and disclosure of information can occur without explicit interaction or oversight.

Moreover, these applications originate from needs and goals that are independent of this work, and thus provide a more realistic test bed for the design method.[34] In both cases, I was able to influence the design of the system based on considerations originating from the proportionality method during subsequent design iterations.

The ability to study exogenous projects enables access to a very large design scope. In particular, deployment-quality software requires significant resources, which only the collaboration of large research and development teams can provide. This model results in increased efficiency, as I concentrate only on the specific aspects of interest (privacy, security, and the design method). In the Personal Audio Loop study, software development and execution of user studies were in large part performed by others. Reno was largely developed by a team of programmers at Intel Research.

The two case studies also target different user groups. The Personal Audio Loop is a personal, portable device that records rich information (audio conversations) for a short period of time; it impinges principally on the privacy of the secondary stakeholders of the application. The Personal Audio Loop is an example of *capture and access* systems, which are at the base of many ubicomp applications [169].

Reno is a personal location disclosure application targeted at small social groups that handles semantically dense information (the user's location). It is a peer-to-peer messaging application, in which information is not captured and stored, but can be transmitted to other individuals.

[34] The Personal Audio Loop originated from an idea by Truong and Abowd, and was developed and evaluated through a collaborative effort involving Hayes, Patel, Kientz, Farmer and me. Reno was a design originally proposed by Smith, Consolvo and others at Intel Research, and its development and evaluation involved a large group of researchers including me.

4.3.1 Personal Audio Loop

I describe here how the proportionality method aided the development of the Personal Audio Loop (PAL), a personal, portable, audio memory aid device. An overview of the design process is available elsewhere [87, 101]. The main characteristics of this application and case study are the following:

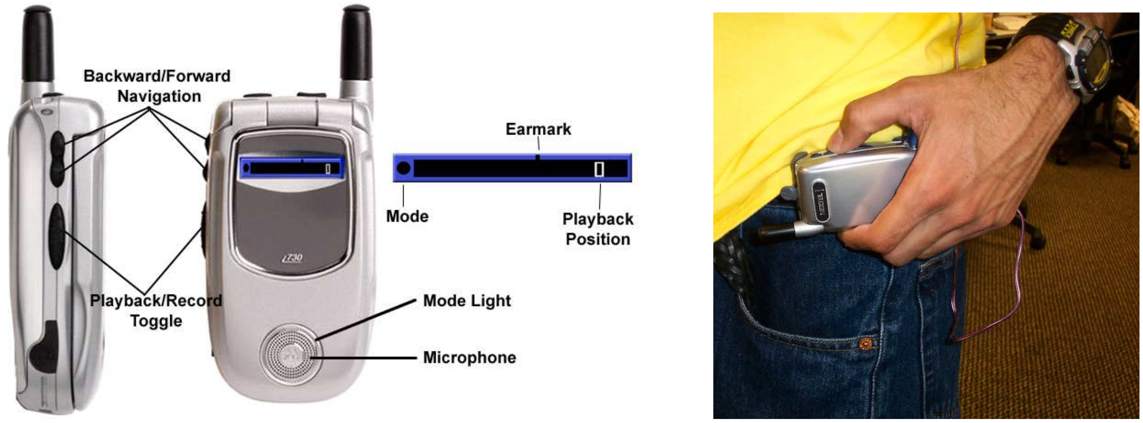
- PAL is a personal and portable capture and access application.
- PAL may impinge on the privacy of secondary stakeholders (the conversation partners of the user and unrelated passersby), leading to adjudication issues.
- The proportionality method helped identify further research questions, and provided guidance at specific moments during design.

4.3.1.1 Design

PAL was motivated by the everyday experience of conversational breakdowns, as people try to remember something that was said in the recent past, such as the topic of a conversation before being interrupted, or a name or number briefly heard in situations of high cognitive load. The device (Figure 4.3) allows the user to replay, at any moment in time, any sound that was heard in the recent past, up to a defined maximum time span, or *buffer length* (for example, up to 1 hour in the past). Sound is stored in a circular buffer: audio older than the buffer length is overwritten automatically and cannot be replayed. PAL is integrated onto a cell phone, but the device only records sound from the environment, and not phone conversations. Users can replay recordings, rewind and fast forward through them or jump to bookmarked positions (“earmarks”). The stored audio can be heard either through the loudspeaker on the phone, or through the external speaker/mike. When the device is recording, a red LED lights up on the front of the phone casing.

4.3.1.2 Analysis

Our own experience and informal conversations with others suggested that this service could be helpful in numerous everyday situations to various categories of users,



(Figure by S. Patel).

Figure 4.3: The Personal Audio Loop: the device and its usage.

such as busy professionals. The designers were also acutely aware of the potential concerns people could raise, knowing that a device was constantly recording their conversations.

We thus set out to analytically study how the service would be used and its potential adoption issues through 1) a laboratory study to probe interface usability, 2) a diary study targeted at understanding why, when and how people would find PAL useful, followed by interviews and targeted surveys, 3) a legal survey, 4) a deployment over several weeks and 5) a survey of communication partners' reactions.

While I am not in the position of providing legal opinions on this design, I mention that a preliminary assessment found that PAL falls into a gray area of EU data protection law (Directive 95/46/EC), and might comply with it given a favorable DPA opinion, whereas strict interpretation of surveillance and wiretapping legislation in states of the US with "two-party consent" (*i.e.*, all parties present at a recording must consent) might directly challenge the application's legality. Clearly, these results are inconclusive: to reach more reliable assessment of the acceptability of PAL, information from more focused user studies is necessary, as discussed below. Specifically, legal analysis suggested to focus on notification mechanisms and on expectations of privacy.

In the following analysis, I adopt a utilitarian (as opposed to principle-driven) stance towards design [164]. Moreover, I assume that the implementation is trusted, *i.e.*, that the implementation addresses standard security issues such as tampering with application code or installing unauthorized software.

Desirability

This analysis was approached at two levels: the usefulness of the memory aid was assessed by deploying a diary study; these results were confirmed during a brief deployment. The diary study results suggested that participants would use the application often (avg. 3.5 times per week) and for relevant purposes (the top three being to remember forgotten details of conversations, replaying conversations to their conversation partners, and recovering the topic of a conversation after an interruption), with a significant and positive effect on their daily activities.

The deployment of four PAL prototypes confirmed that participants used PAL approximately as often as they had indicated in the diary study. Moreover, they reported adopting self-regulating behaviors (*e.g.*, disabling the device in specific circumstances.)

Questions were raised during early design regarding the burden imposed on conversation partners and third parties; during deployment, in most cases, conversation partners did not object to the use of PAL after the user explained its purpose and characteristics (*i.e.*, the limited retention time). However, users also reported not always informing conversation partners of the presence of PAL, to avoid explaining its features repeatedly. In some social settings, they both avoided mentioning and using the device altogether, or they turned it off spontaneously, while in other cases they used it but did not discuss it.

Users may adopt reasonable self-regulating behaviors with regard to their conversation partners' privacy. However, the small scale of the deployment left open two fundamental questions of adjudication raised by the desirability and appropriateness analyses of the proportionality method. The first question relates to whose interests should prevail.

The primary stakeholder (the user) of the application may have a legitimate interest in using PAL, for example due to a memory dysfunction or simply because of cognitive stress imposed by his or her occupation. This interest may be opposed to that of secondary stakeholders or third parties (who might not want to be recorded, even if only temporarily). The second adjudication question relates to the proportion of individuals opposed to the application. If only a small minority of secondary stakeholders and third parties oppose PAL and the vast majority does not care, should we yield to the contrary minority and curtail a large market potential?

In this case, to make any such determination we needed to understand *to what degree*, and *in what situations* secondary stakeholders are most likely to object to the use of a device that can potentially cause the recording of their conversations (*i.e.*, are objections unqualified or do they depend on the location, on the topic, on the identity of the conversation partner, or on the perceived confidentiality of the conversation?)

Limitations of the prototypes prevented us from thoroughly investigating these questions through a long-term deployment that may have provided strong qualitative and quantitative evidence. Therefore, we organized an event-contingent Experience Sampling Method (ESM)[35] study to probe this question, in which three investigators asked all their conversation partners, during the course of their daily activities, to imagine that the investigator had been using PAL, and to state their opinion and feelings about this use [101]. This study was called the PAL Proxy study. In the PAL Proxy study, human 'proxies' (of the researchers) administered short questionnaires to the people with whom they talked during their ordinary daily activities. The questionnaires asked conversation partners to

[35] Experience Sampling is a self-reported inquiry technique, that has been used within behaviorism, medicine, and industrial psychology starting in the 1960's [181]. There are many variations, but the basic idea is that a participant is asked to keep track of his or her feelings or behaviors, at specific times, normally during a time span of days to weeks.

suppose that the ‘proxies’ had been using PAL in the preceding conversation, and to respond to a short set of Likert questions on the acceptability of the application from their points of view. The questionnaires could be completed instantly or mailed to the investigators later (see Figure 6.2 for a photograph of the Proxy questionnaire).

The participants of that study expressed a desire to be informed and asked permission before using PAL. Yet, in most cases, they reported not being likely to ask the user to erase the recording after the fact. I concluded that PAL would pass a desirability judgment, if the user had a need for a memory aid, the setting of use could sustain the residual risk of misuse, and, most important, if the secondary stakeholders had sufficient awareness of this application.

Appropriateness

I claim that the proposed technical solution (*i.e.*, open mike audio recording on mobile device) is the most cost-effective. I considered alternatives such as:

– installing microphones in the environment and transmitting digital audio wirelessly for recording on devices worn on the user’s body and

– fully infrastructural, off-body, recording and storage.

Furthermore, continuous operation is necessary because PAL, as a memory aid, is useful exactly when one does not expect it; if the user had to trigger the recording intentionally, then PAL would not be any different from a pocket tape recorder, and it would not provide the unique benefit that users found so compelling.

The application is not modifiable by the user and does not allow the storage of the recording past the buffer length time. During deployment, we discovered that users had found a way around the retention time limitation by indefinitely pausing the recording. This emergent use showed that the users had a strong need for a audio notepad, in addition to a memory aid; however, consistent with the proportionality assessment, I asked that this re-purposing feature be removed from the final version of the device. We also discovered that participants were using PAL to relay information between different conversation partners, and for proving points in discussion (*e.g.*, *"you said that…"*); in my opinion, these unexpected and potentially disruptive uses could be curbed by a combination of social pressure and retention time reduction. These observations in my view confirm that real-world evaluation of ubicomp technologies within a cyclic development process is indispensable for controlling emergent or co-evolved behaviors, on legal and ethical grounds.

A technical analysis aimed at finding alternatives for reducing the burden on conversation partners' privacy did not provide any further solutions. In addition, I did not find a way, with a comparable cost and effort, of achieving the same application goals without employing a technological solution.

In summary, I assessed that the selected technical solution would be appropriate for meeting application goals, although our observations raised the issue of trust between the user and his or her conversation partner with respect to an invisible technology.

Adequacy

A list of relevant interface affordances and information policies was derived through iterative analysis by three expert designers (see Figure 4.4).

For each feature, I identified acceptable design ranges according to steps 3 and 4 in the adequacy process (see Table 4.1 and Figure 4.2), along with the affected stakeholder and a justification. The table shows the compromise reached between the success criteria and stakeholders' privacy concerns, and is the outcome of design iterations aimed at justifying a value for each variable. Italic font is used to indicate the relevant stakeholder. Justifications are provided in parentheses. Some features can be adjusted within constraints (*e.g.*, feature 1), while others are fixed due to the limitations of the selected technology (*e.g.*, feature 3). Moreover, features can be expressed in different ways: microphone range can be measured in meters, but for this purpose it is more helpful to use proxemics categories (*i.e.*, intimate, personal, social, public [84]) or to reference human sound perception.

This analysis raised a fundamental question of contextualization, which is a general problem for technologies operating in an automatic fashion. The question is whether and how the social and technical environment can affect the use of the application. If different privacy requirements could be associated to specific circumstances (*e.g.*, when driving alone), and at least part of these circumstances could be detected by a recognizable context, this could bring about significant design implications, as suggested by the work of Hong and Landay [91]. This observation led to investigating *what application parameters* (*e.g.*, retention time) we could adjust to meet a compromise between the interest of the primary users and conversation partners.

1. Microphone range; expressed as a spherical space which can be modulated in continuous manner (characterization is indicated in short form below).
2. Buffer length and retention time (in PAL the two variables are joined); continuous variable, in time units.
3. Access and browsing facilities; selection of (tape-like browsing, skimming, *i.e.*, replaying at faster speed).
4. Audio output channel; selection of (headphone, external loudspeaker).
5. Ability to set “bookmarks” at significant moments in time to facilitate search; selection of (yes, no).
6. Permanent audio storage; selection of (yes, no).
7. Activity notification cue to the conversation partner; selection of (visual, audio, none).
8. Placement of the microphone relative to the user; selection of (any location where the device can be attached to the body or clothing, or headset connected to device; headset in clothing or apparel).
9. Appearance of the mobile device; selection of (any mobile recording device).

Figure 4.4: PAL Design Features.

Table 4.1: PAL Adequacy Analysis.

Feature	**Critical success range (step 3)**	**Privacy desirable range (step 4)**
1 mic. range	arm's length, *i.e.*, approx. 1*m* (from diary study and deployment)	*conversation partners and unrelated individuals*: 1*m* (from proxemics literature and survey of diary study participants)
2 buffer length	10*min* – 1*hr* (from diary study and diary study participants survey)	*conversation partners*: 15*min* (the experience sampling privacy survey suggested that *retention time* could be much longer, up to a week or more) *primary user*: 1*hr* (designers' choice: this time is sufficiently short to reduce risk of abuse in case of theft or loss)
3 access facility	tape recorder-like browsing (lab user study and deployment show that skimming is impractical due to device performance limits, that browsing is efficient enough and that there is no desire for visual search)	*conversation partners*: tape-like browsing (this is a designers' choice: tape-like browsing is the method that requires most effort to access stored information. By increasing access cost, access is reduced, to the benefit of other's privacy)
4 output channel	headphone and external loudspeaker (this is a forced choice: technical limitations do not permit to block headphone use with PAL)	*conversation partners*: only external loudspeaker for sound output; this increases visibility and thus participation and enables consent dynamics. *primary user*: headphone or external loudspeaker (the user wants to listen without other people overhearing the recording)
5 bookmarks	no (deployment shows that bookmarks are not essential for using the application)	*conversation partners*: no (designers' choice: bookmarks would allow users to access stored information too easily)
6 storage facilities	no (deployment shows that users use the application even without permanent recording features)	*conversation partners and unrelated individuals*: no (designers' choice: allowing permanent archival would heighten the risk of abuse)
7 notification cue	visual (this is a non-intrusive cue, and it has been shown to be acceptable by users during the deployment)	*conversation partners*: visual (this is designers' choice which has not been verified with an actual user study. However, designers assume that an acoustic cue would be too intrusive.)
8 microphone placement	speakerphone microphone and cell phone unit worn on belt clip (this is one of numerous locations used by participants in the deployment of the device)	*conversation partners:* in a visible position (this is a designers' choice not verified with an actual study. As with feature 7, the visibility of the device is supposed to favor consent dynamics.)
9 device appearance	cell phone (device must be mobile, and users do not want to carry an extra device)	*conversation partners:* audio recorder (cell phones are not associated to recording functions); *deployment condition*: the user is ultimately responsible for its appropriate use.

In the Proxy study mentioned above, we asked participants to indicate for how long they would allow the user of PAL to retain the conversation's recording (*i.e.*, to estimate its *retention time*). Participants stated that they would allow the user of PAL to retain their conversations for much longer than we had expected ("at most one week" or "as long as they need it" in most cases). However, they strongly asserted their desires to be asked permission before the user replayed the conversation to another person or copied it to another recording device. These results suggest that the participants did not express their concerns and needs in terms of retention time, but rather that the focus was on misuse and social appropriateness. In this case, a straightforward, quantitative "balancing" of retention time might not represent an acceptable solution.

4.3.1.3 Policy and Management Provisions

A variety of security management options can be adopted by the manufacturers or service providers of PAL. I consider three such options: increasing knowledge about the application[36], limiting use to specific user groups and deciding not to market the application.

Previous research has suggested that the use of privacy-invasive technologies, especially between individuals, fits within a boundary negotiation process [143]. This negotiation does not need to be explicit, but may take the form of self-restraint, and is meaningful only if all individuals are aware and knowledgeable of the device. Consider feature 9: on the one hand, PAL users do not want to carry extra devices; on the other hand, cell phones are not usually associated with audio recording. The case is similar to the recent appearance of "camera-phones." Unable to reach a compromise over this design variable,

[36] This mirrors one of Altman's conclusions in the book *The Environment and Social Behavior* [20, p. 213]. This point also affects the legal test of "technology in common use" adopted by the US Supreme Court in the Kyllo case.

I derived a deployment condition from feature 9 (“the user is ultimately responsible for its appropriate use”) that should be assessed through summative evaluation.

A second option for reducing the potential negative implications of applications such as PAL is that of limiting its use to certain categories of users. Given that PAL may be mostly useful for people with memory disabilities, a certification of such disability might be required for acquiring and using this application. While this happens with numerous other technologies (*e.g.*, operating vehicles) the administrative costs imposed by a licensing scheme would most probably be excessive, in relation to the potential harm that this application may pose, and the profits generated.

Finally, manufacturers may opt not to deploy certain applications at all, in an effort to reduce liability risks. In the case of PAL, this choice may be exceedingly precautious, given that audio recording devices are readily available, which are much more invasive than PAL.

4.3.1.4 Contribution of the Proportionality Method

The proportionality method benefited the analysis of PAL in four ways. First, it provided a reasoned basis for discussing a very controversial application. Applying the proportionality design method to this application allowed us to formulate a solid argument in favor of the usefulness and acceptability of PAL, given specific safeguards and conditions on its use (*i.e.*, public awareness and strong need). This result was not granted from the beginning: the initial proposal for this application was met with much skepticism by other researchers, both regarding its legality and user acceptance.

Second, the proportionality method offered a detailed analysis of application acceptability in the absence of regulatory guidance. Legal analysis was prompted in the quest for answers to issues raised during design. Legal analysis, while failing to provide conclusive guidance, indicated potential pitfalls and liability concerns for this application.

Third, it gave an indication of what research steps to conduct further. After the initial evaluation, a specific study evaluating the acceptability of PAL by conversation partners was performed (the PAL Proxy study mentioned above).

Fourth, the proportionality assessment did influence the definition of application requirements (such as buffer length, or the need for a visible indicator light) and indicated how designers should react to unexpected adoption events, such as the case of the users finding a way to extend the retention time: that feature was removed from the design as it was deemed incompatible with the assumptions justifying the proportionality argument.

4.3.2 Reno

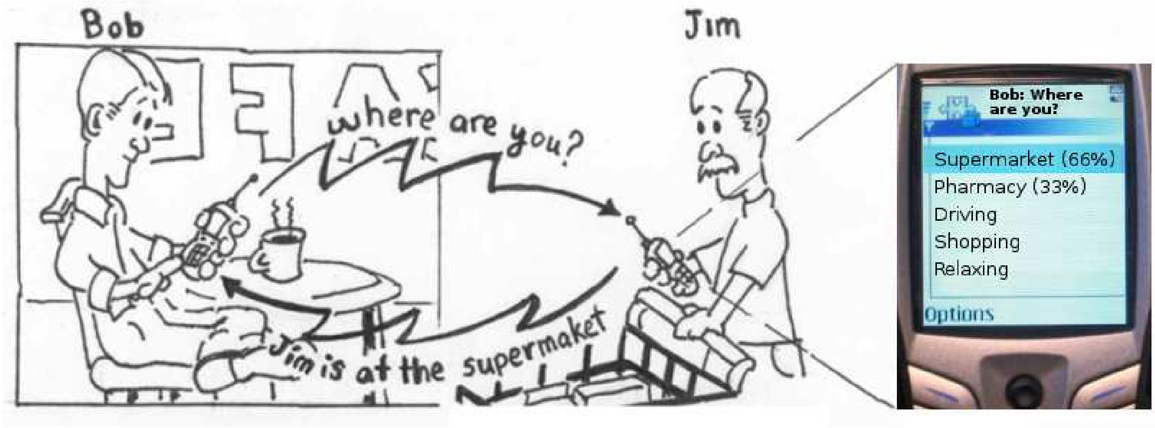
In this section, I present an analysis of Reno according to the proportionality method. The characteristics of Reno are the following:

- Reno is a symmetric, peer-to-peer application;
- Reno is a *social mobile application*, designed for small social groups;
- Reno has an intentional control structure (except for the automatic functions).

Specific decisions regarding the design of Reno and the questions to probe with the user study were driven by the considerations of desirability, appropriateness and adequacy. These decision points are highlighted below.

4.3.2.1 Design

Reno is a location-enhanced application that allows the user to request the location of other users and to reveal his/her location to them. The application runs on Nokia 6600 phones. Before using Reno to disclose a location, the user must define place names (*e.g.*, "School" or "Home") and assign them to physical locations. When a place name is defined by the user, it is associated with the current location, sensed using cell tower connection patterns, similar to the technique described by Laasonen *et al.* [115]. The program will offer the name each time the user subsequently visits that location, to relieve



(Drawing by K. Truong)

Figure 4.5: Usage Scenario for Reno.

The application presents a list of likely locations and a static list of activities when replying to request.

the user from typing it again. When sending a location, either as a reply to a request or by the user's initiative, Reno offers a selection of nearby place names, as computed by the location algorithm. Reno also provides a customized, pre-defined list of activities that may be used instead of place names for replying to messages as a fallback option (in the figure: "Driving," "Shopping," "Relaxing"). As a privacy-enhancing feature, the physical location (cell tower) of the user is never sent by Reno: only the user-defined place name is sent (Figure 4.5).

Reno has two automated features: the Instant Reply List and Waypoints. The former causes Reno to reply automatically with the current most likely location to any request coming from a person on the Instant Reply List (a user-defined list). If the location is undetermined, Reno transmits "Unknown Location."

Waypoints cause Reno to trigger a location disclosure when the user enters a specific, pre-defined location. To set up a Waypoint the user must indicate both the location of interest (*e.g.*, "Office") and the recipient of the message (*e.g.*, "Bob"). Each time Reno senses that the user arrives at the "Office," it will send a notification to "Bob." To avoid bursts of messages when the user briefly leaves and returns to the same location, there is a two-hour timeout. Users can view a list of how many times Reno disclosed their location automatically using an audit tool called the Activity Report.

Reno uses SMS messages to communicate. The messages consist of two parts: a human-readable sentence, followed by compressed information, a checksum and a 'magic' string used for message recognition. Human-readable messages increase the opportunities for using the application with people not using the software.

4.3.2.2 Analysis

The requirements analysis of Reno exposes information management issues typical of the management of personal privacy, which were identified early by the designers of the application. These include:

- prevent unauthorized parties from obtaining users' location information;
- prevent the disclosure when the user is in certain locations (*e.g.*, locations that are 'undesirable');
- prevent disclosure under other conditions (*e.g.*, time of day, frequency of requests);
- avoid disturbing the user with disruptive messages;
- limit the management burden of configuring and auditing automatic functions.

These privacy goals were considered during the design and evaluation of Reno. The design alternated two design cycles with three user studies: an Experience Sampling Method (ESM) study, a pilot study and a longer deployment with external users.

The ESM study was performed prior to the design of a first version of the application. The goal of that study was to understand to whom people were willing to disclose their locations and at what levels of detail [51]. Participants shared different levels of detail about where they were, based on: who was asking, what the participant was doing, and why they thought the requester wanted to know. Furthermore, they did *not* 'blur' their locations (*i.e.*, share a level of detail that is true but vague, such as the city name instead of the street address) in an effort to protect their privacy. And finally, participants expressed a need to be able, on occasion, to "stretch the truth" about their locations, for various reasons. All these findings suggested to allow user-selected names for location, instead of geographical coordinates.

Following that study, an initial application prototype was developed and a short pilot study was conducted with the same researchers to inquire the usage patterns of the application [158]. The prototype used in this pilot study did not include the Instant Reply List and Activity Report features described above, but did include Waypoints. Participants used location as a proxy for many other things (*i.e.*, revealing location information carries contextual knowledge, regarding the person's activity, plans and movements). So, in the second design of the application, I suggested introducing the ability of sending an activity (*e.g.*, "driving") instead of a location. This feature has repercussions on information control and privacy. Also, automatic features, if they are employed at all, must be designed very carefully (the Waypoints in this version of Reno suffered from excessive false positives).

With the experience gained from the pilot study on how participants used location to communicate plans and activities, I structured a second deployment to address the privacy questions raised by the proportionality method. The version of Reno used in the second study incorporated all the automatic features described above, including the Instant Reply List and the Activity Report (the audit system for the automatic functions). Proportionality suggested probing two issues of relevance:[37]

– Given that the purpose of automatic features (Waypoints and Instant Replies) is to minimize disruption and management burden, what is the design balance with the loss of control ensued by these features?

[37] These two research questions were chosen as the result of an iterative selection process, from a dozen issues of relevance, and a shortlist of four (management burden; performance of automatic disclosure mechanisms; support for plausible deniability and deception dynamics; use of Reno as a tool enabling high-level activities.) [95]

– Is the documented need to tailor location disclosures (and potentially deceive) supported by the application [54, 85]?

This deployment involved two groups of teenage and adult participants. These users were selected to expose potential tensions between practical dependence and aspiring independence of teens in relation to their parents [109, 113]. I identified three stakeholders in this application: the disclosing party or user, who operates Reno to disclose his or her location; the requesting party, and the location service provider (I ignored the telecommunications operator in this analysis).

Desirability

Assessing the desirability of this application rests on the observation of similar applications already in the marketplace, such as AT&T Find People Nearby [24] and Dodgeball [4], as well as market research data [165] suggesting that people find this kind of application useful. These systems are already in use, so privacy risks are not so grave as to prevent deploying the application, contrary to the PAL case. Existing applications attest to the application's purpose (*i.e.*, being able to ask others for their geographical location). In addition, experimental data collected in the three stages of this study allows us to make some stronger claims about the usefulness and privacy concerns.

Although the ESM study was not planned following the proportionality method, the research questions addressed within that study allowed the researchers to gather valuable information for making an argument about the usefulness of a location disclosure application. Specifically, the questions of *how* people decide whether to disclose their location, and *what* to disclose relate to the needs of the disclosing party (see Table 4.2). The question about the usefulness of the application to the requesting party was addressed in the study by asking participants, in a subset of the ESM samples, whether they would have liked to know others' locations at that moment. These results should be taken with caution, since the simulated requests were not initiated by the user and lacked social consequence, but they constitute an indication of the times the users might have used the

Table 4.2: Reno ESM study research questions and mapping with legitimacy.

Proportionality	ESM Research Questions	ESM Results
What are the needs of the disclosing party?	Do people want to disclose their location?	Yes
	How do people decide whether to disclose their location?	Users decide based on who is asking, and the reason for the request.
	What do people want to share about their location?	Users disclose either the most useful information or nothing.
What are the needs of the requesting party?	Do participants want to know about the location of others?	Participants would have liked to know another person's location approx. 1.6 times a day. (They were asked this question 5 times a day).

system for requesting other's locations. Such indication was confirmed during deployment.

Evidence from the ESM study supports the desirability of this application, as long as the user is informed that location information is being collected and disclosed about him/her. Clearly, this condition directly pertains to the issue of automatic disclosures, as discussed below.

Appropriateness

Recall that the appropriateness stage requires to assessment whether a specific technological implementation meets the best compromise of cost, privacy and security risks and performance, whether it can be misused and if the same application can be accomplished without the technology. There are several ways location information can be communicated between individuals.

The purpose of Reno is to lower the cost of revealing location in a mobile setting, streamlining communication. The version of Reno described above is a peer-to-peer system using cell phones that communicates via SMS messages. An alternative option is a server-based system that uses cell phones as terminals (AT&T Find Friends and Dodgeball are both in this category, although with different architectures); this introduces, however, a third stakeholder with potential multilateral security implications.[38] Yet another option would be to use a different location or communication technology altogether, similar to child-tracking devices that use GPS and operate without control by the user; this kind of surveillance however was deemed too invasive and costly. Overall, Reno's peer-to-peer architecture seems to provide a good security compromise. A second issue is whether to disclose the user's location automatically, without his or her knowledge. To answer this question, I specifically designed the third user study to probe whether automatic disclosures are acceptable and can be used with audit mechanisms to curtail misuse of location information. These participants did not display a strong need for automatic functions, and this induced us to question the need of automatic disclosures.

Message traffic between mobile phones could be intercepted by eavesdroppers and telecommunication providers. Based on mainstream security assessments, I assume this risk to be low; telecommunication providers are considered trusted for the purpose of this application, given specific legislation protecting the confidentiality of communications. The software used to generate and transmit the location descriptions runs on the user's phone and is always under his/her physical control. Also in this case, I assumed a

[38] The question is whether service providers need to process or retain records of the location information of users of a system like Reno. In this case, thanks to the great interest in Location-Based Services (LBS) in the past few years, legislation provides strong guidance. EU Directive 2002/58 permits storing the user's location only if the information is necessary for providing specific services to the user [3, §9], and requires informed consent. In the US, the Electronic Communications Privacy Act (ECPA) [8] and FCC regulation requires informed consent for the disclosure of location information to third parties and for its use for value-added services [64]. Therefore, if location information is managed by the service provider, informed consent and specific security safeguards are required in both major markets. The peer-to-peer architecture of Reno reduces data protection and management costs for the service provider.

1. Visibility of location requests in Reno’s main screen; selection of: (visible, non visible).
2. Instant Replies, *i.e.*, Reno responds automatically to requests; selection of: (implemented, not implemented).
3. Restriction of Instant Reply to specific individuals; selection of: (none, buddy list).
4. Waypoints; selection of: (implemented, not implemented).
5. Configurability of IRL, based on selection of: (location, time of day, date, none).
6. Configurability of Waypoints, based on: selection of: (time of day, date, none).
7. Are instant replies are sent from locations that are not labeled; selection of: (do nothing, send a message with “Unknown Location”).
8. Where to put audit information about disclosures Reno sent automatically; selection of: (main screen, separate screen, none).
9. Type of location information transmitted; selection of: (geographical coordinates, urban coordinates, user-defined label, centrally defined label).
10. Ability of transmitting activity as well as location; selection of: (yes, no).

Figure 4.6: Reno Design Features.

reasonably trusted software implementation. Reno could be abused by third parties who repeatedly query the user’s location, with the objective of “stalking” him or her. This concern might be especially problematic in the case the disclosing party feels compelled to reply due to social pressure (*e.g.*, the requesting party exerts some form of social authority). However, in our deployment, participants indicated that they would expect others to conform to self-regulating social practice in requesting locations, especially because requests would be visible to the disclosing party, and did not express such concern.

Currently, individuals communicate their locations while mobile by phone or SMS. Reno is intended to replace potentially lengthy and disruptive phone calls, and hard-to-type SMS messages. Non-technical solutions to this application problem were not identified. Technical alternatives included SMS templates. However, templates are much more cumbersome than Reno because the user would have to type the location manually. Concluding, a peer-to-peer system that operates with the knowledge of the disclosing party seems to provide a reasonable compromise.

Table 4.3: Reno adequacy analysis.

Feature	**Critical success values**	**Privacy burden desirable range**
1 visibility of requests	*disclosing party*: no constraint (the deployment suggests that the amount of requests visible on main screen is not excessive)	*disclosing party*: visible
2 instant replies	*disclosing party*: not implemented *requesting party*: not implemented (deployment participants indicated lack of confidence in automatically disclosed information)	*disclosing party*: not implemented (automatic disclosure causes a loss of control)
3 restriction of instant replies	*disclosing party*: no constraint (see variable 2)	*disclosing party*: yes (designers' choice—avoid risk of unauthorized disclosure)
4 waypoints	*disclosing party*: not implemented (deployment participants did not indicate strong need for, nor confidence in, waypoints)	*disclosing party*: not implemented (deployment participants indicated that the waypoint feature might result in unintended disclosures, and might disturb the recipient)
5 instant reply config	*disclosing party*: no constraint (see variable 2)	*disclosing party*: time-of-day, location (this is a designers' choice: this configuration options increase control on disclosed information)
6 waypoints config	*disclosing party*: no constraint (see variable 2)	*disclosing party*: time-of-day (this is a designers' choice: this configuration option increases control on disclosed information)
7 instant reply in unknown location	*requesting party*: yes (this is a designers' choice: providing a message in unknown locations would improve the disclosing party's visibility and perceived reliability of the application)	*disclosing party*: no (this is a designers' choice: this feature increases ambiguity, supporting plausible deniability)
8 audit info. location	*disclosing party*: separate screen (this is a designer's choice: this information may clutter the application main screen)	*disclosing party*: main screen (deployment participants never accessed audit information in a separate screen)
9 type of location information	*disclosing party*: no constraint *requesting party*: no constraint	*disclosing party*: user controlled label (deployment suggests that participants liked the freedom to tailor what Reno communicates about them)
10 activity disclosure	*disclosing party:* yes (deployment study participants reported that it was useful to communicate their activity instead of their locations) *requesting party:* no constraint (this is a designers' choice)	*disclosing party:* yes (deployment study participants suggested that more flexibility supports evasive answers; this is confirmed by literature [100])

Adequacy

The design features impacting the privacy of Reno's disclosing party emerged during the design process, in the form of decisions we had to make during design (see Figure 4.6). In a similar fashion to the discussion of the Personal Audio Loop, acceptable design ranges according to steps 3 and 4 in the adequacy process were identified (Table 4.3). The stakeholder are indicated in italics and the related justifications are in parentheses. It should be noted that design features 3, 5, 6, 7, and 8 became irrelevant once a determination was made to forego automatic functions.

4.3.2.3 Contribution of the Proportionality Method

The application of the proportionality method resulted in two significant contributions and highlighted potential challenges. First, it suggested research questions probing the acceptability of automatic disclosures and whether the application could be used in dynamics of denial and deception. Although proportionality suggested to probe these questions, the outcomes of the study did not coincide with our expected hypotheses. Regarding the first question, we had hypothesized that participants would have managed to handle well the automatic features. Instead, these participants indicated that automatic functions were in fact not very useful to them. Although participants did not cite privacy as the primary concern affecting their need of the automatic functions, the results tipped the balance of usefulness and privacy towards the protection of privacy. The second question we probed, that deception and denial practices could occur with this application, was supported by direct observations made during the deployment and by evidence that participants would have been able to exercise plausible deniability if necessary. These findings provided solid grounds for increasing control over location disclosure and preserving the abilities of users to label their own locations. Thus, specific design and evaluation decisions were made within the proportionality process. The development of social mobile applications at Intel Research has continued with a map-based version of the application [100].

Second, this case study showed that even in cases in which the method is applied late in the development process of an application, it still can be valuable. I entered the project after the second study, and proposed several suggestions both for the application design and for future evaluation steps. I integrated evidence gathered by user studies that were not planned as part of the proportionality design method. I used evidence from those studies to argue about user needs and drive successive evaluation and design. Thus, it is not necessary to plan an entire process according to the proportionality method; data already collected can be integrated into an assessment according to the proportionality method, along with information collected for that specific purpose.

Deciding what application should be the target of the evaluation with the proportionality method is a challenge tightly connected with the relationship of summative and formative evaluation in exploratory design. There are two methods to select an application target of an evaluation. The first method is to select the broadest option that supports the application goals; this should be used for exploratory designs. In the case of Reno, this would have described the application as a location-enhanced messaging system, without further constraints. The second method of selecting technologies is that of selecting one specific design, as was done in this case. For example, I described Reno as an application that can automatically respond to others' with the user's location and that enables users to define and label their location (as opposed to sending geographical coordinates). This more detailed description of the application allows designers to reach more precise assessments, but constrains the design space (*i.e.*, the scope of the appropriateness judgment).

Finally, this case study also hinted at the potential limits of interpreting design as a tradeoff between burden on privacy and application benefits. While such tradeoff is typical of legal and policy analysis, it does not fit well for applications, like messaging systems, based on intentional interaction. For example, while the automatic features in Reno can be analyzed using a benefits/burden approach, the effects on interpersonal communication (including privacy and security) of other design features such as the subjective labeling scheme of locations are not so quite straightforward to evaluate using simply benefits and burden.

4.4 Conclusion

In this chapter, I introduced the principle of proportionality and the design method I developed from the principle, to aid the analysis of security and privacy issues in ubicomp applications within a user-centered approach. I showed how the proportionality method has been used for analyzing two different applications, and how it contributed by leading the designer to further evaluation questions, specific design choices and the evaluation of broad alternatives. An obvious question at this point is whether the proportionality method helped the analysis of these applications or whether the determining factors were the knowledge and experience of the person applying it, *i.e.*, me. I investigate this question in the next Chapter, with a semi-quantitative evaluation of the design method’s performance.

CHAPTER 5

THE DESIGN METHOD EVALUATION

The experience gained in the two case studies of Chapter 4 suggests that the proportionality method may increase the coverage of security and privacy requirements analysis and improve overall design quality. To understand whether the design method is usable by others and whether it provides an actual benefit in terms of design quality, I tested the method with other designers. The evaluation of the method's performance sheds some light on these questions, and shows where research in this field might proceed next.

Evaluating the performance of design methods is inherently imprecise, because, even with large pools of participants, it is difficult to control external variables such as prior experience and spur-of-the moment insight. Designing artifacts is one of the most intellectually challenging and idiosyncratic of activities: the difficulty of proving a design methods' effectiveness and utility may explain in part why these tools rarely enjoy widespread popularity, even in well-established fields.

Over the past few years, there have been several attempts at creating methods or guidelines to addressing the privacy and security of design ubicomp applications. Some of these methods have been mentioned previously, including Jiang *et al.*'s proposal of using economic and information theories to modulate flows of personal data [110], Bellotti and Sellen's framework of feedback and control [31], Hong *et al.*'s risk analysis process for ubicomp [92] and Chung *et al.*'s set of design patterns for ubicomp [45]. To my knowledge, Bellotti and Sellen's framework has not been formally evaluated in the domain of ubicomp, nor has Hong *et al.*'s.[39] Only Chung *et al.*'s design pre-patterns have been evaluated, albeit unsuccessfully. Their design pre-patterns were developed through iterative refinement and tested in a design study involving both experienced and inexperienced designers. Among general patterns were also 15 patterns specifically aimed at the privacy issues in ubicomp. However, Chung *et al.* reported that the evaluation participants did not use the design pre-patterns in any meaningful way to complete the design exercises that were proposed. According to these researchers, this might have happened because the proposed patterns were too abstract, privacy issues were not emphasized enough in the design exercises' briefs, and in general because patterns might not be suited for addressing non-functional requirements such as privacy [45]. Learning from their experience, I attempted to test specific procedural guidelines and to focus on the evaluation of privacy and security.

This Chapter includes the evaluation of the proportionality method, which first involved six volunteer graduate students in the *Information Security Policy* class held at this Institute during Spring 2005 (the Pilot Study). Then, a larger-scale evaluation involving 48 graduate students in the *Introduction to HCI* class held in Fall 2005 was conducted (the Design Method Evaluation Study). In the second evaluation, I chose to evaluate the proportionality method against two methods cited above, namely Hong *et al.*'s Risk Analysis and Bellotti and Sellen's Feedback / Control framework.

5.1 Pilot Study

The pilot study was performed to evaluate the comprehensibility, usability and stability of the proportionality method across designers and to test the evaluation process in view of a larger study. The study was conducted with six graduate students. Students

[39] J. Hong, personal conversation.

were given the option of using the proportionality method for completing a semester-long design exercise. They were asked to design a ubiquitous computing application of their choice amongst two options. I analyzed their written deliverables using quantitative metrics and conducted follow-up interviews. Results suggest that the proportionality method is comprehensible and usable by inexperienced designers. Participants commented that the method may help especially in the design of exploratory applications with diverging stakeholders, broadening the coverage of the design process and generating stronger rationales for design decisions. Also, the results suggest that the proportionality method may increase the thoroughness of requirements analysis.

5.1.1 Hypothesis and Experimental Procedure

The objective of this study was that of verifying the following two hypotheses:

1. the proportionality method is understandable to and usable by inexperienced designers.
2. Inexperienced designers reach similar conclusions as experienced designers. Specifically, they identify the same main design issues and reach similar conclusions on these issues as the expert designer (me).

I recruited three groups (of two students each) of volunteer Master’s students in the CS6725 Information Security Policy class at our institution. I asked these participants to perform a design exercise using the proportionality method as their semester-long project assignment for the class. Emails of the descriptions of two projects were sent to the whole class, prior to a lecture in which the actual recruitment was made (this material is provided in Appendix B).

During that lecture, I introduced the general domain of ubicomp, its security and privacy challenges, described the design method and relevant bibliographic and legislative resources. The stated project goals were to design (but not implement) their choice between two ubicomp applications with known privacy and security issues. Participating students were asked to take on this assignment as their main semester-long project. Participants formed three groups of two individuals. I chose to have small groups instead of individuals due to the potentially complex and unfamiliar problem domain and large amount of effort necessary to complete the assignments.

The first proposed project was to design a mobile person finder running on a cell phone, similar to the Reno application, discussed in Section 4.3.2. This application allows users to ask the location of others and respond to location requests. The application supports users in meeting, either in person or by phone, assessing the availability of the other persons, or coordinating joint activities. The project brief (provided in Appendix B) stressed the use of the tool for *personal* use, as opposed to location systems for commercial settings such as logistics. Students were provided some references to relevant resources, including existing systems such as AT&T Find People Nearby and legislation regulating location-enhanced wireless services. Groups 1 and 2 chose this project.

The second application was a system to record behavioral data (including audio and video) of a child in a primary school setting. The system's purpose is to support teachers and other school personnel in recording observations about a child before, during and after critical incidents (*e.g.*, escaping the classroom, temper tantrum). This system is loosely inspired by a system currently being designed by Hayes *et al.* [86]. Group 3 chose this project.

Each group was asked to design (not to implement) the information management, organizational policies and privacy- and security-sensitive aspects of the user interface of a system to support the respective application. The groups were asked to justify their technical and organizational design choices and to reference legislation, local regulation, and other policies as appropriate. In addition, they were encouraged to follow the proportionality design method for the analysis of security and privacy requirements. I provided the participants with the CHI 2005 paper describing the proportionality method [97]. Use of the design method was not mandatory; participants were asked to justify their choices if they opted not to use the method.

Demographic data was collected from participants at the beginning of the study, including their experience with requirements engineering techniques, information security standards, IT legislation and the general ubicomp domain.

Participants had approximately two months to complete the assignment. After one month, each group was asked to make a short presentation (20 minutes) in class about their project progress. They also turned in an intermediate report (*mid-project milestone*), which was not graded nor analyzed but helped ensure that students would be on track with the assignment. Participants were asked to include in the mid-term presentation and deliverables: an initial review of design options, relevant literature, legislative and other resources, and all stakeholders of the application. During their presentations, students also received feedback from other students in the class, the instructor and me.

At the end of the second month, all groups completed a final deliverable in which they were asked to include at least the following items:

- regulatory constraints;
- experience from similar applications;
- description of system design;
- information management policies;
- technical safeguards for securing data and people, including relevant aspects of the user interface (*e.g.*, how the system is operated, accessed, *etc.*);
- organizational measures to be adopted contextually with system use.

I evaluated the design products, by comparing the design documents produced by the students with “expert” reference designs. These expert reference designs were produced by me using design material derived from the developers of the specific application. In the case of Reno, I used the basic Reno application, modified after the deployment and my own proportionality analysis. In the case of CareLog, the reference design consisted of the outcome of my analysis of an application similar to the CareLog application concept developed by Hayes *et al*. [86]. These reference designs were written before participants completed any project deliverables.

After the end of the course, I interviewed participants to understand how they had used the proportionality method. This semi-structured interview included questions pertaining to the understandability of the description of the design method (*i.e.*, the published paper [97]); its application (including a subjective assessment of time required to complete the assignment and the impact on the quality of the end product); the resources they had accessed during the design, and questions on specific design choices. The interview lasted between 30 and 45 minutes and was conducted one group at a time. It was audio-recorded and subsequently transcribed. The participation in the interview was voluntary and separate from the rest of the study (all six participants chose to take part in the interview). Because the interview did not provide credit for the class curriculum, each participant received a USD10 gift card for participating.

5.1.2 Demographics

Participants did not have professional experience in ubicomp design. Some participants in Groups 1 and 3 had some professional experience with information security issues. All participants were students of the Information Security MS program at Georgia Tech. Most participants had a technical background, except for one participant in Group 3, who had a technology policy background.

5.1.3 Results

I identified 10 quantitative metrics to evaluate the completeness of the written final reports (I did not consider the oral presentations in this analysis). These metrics are based on the number of occurrences of the following *analysis elements*:

1. expressed threats;
2. usage scenarios;

3. comparisons with existing, similar applications;
4. identified stakeholders;
5. stated requirements;
6. stated design choices;
7. open design issues (that is, design points that were raised by the participants but no conclusion was reached, pending more information or the verification of some other hypothesis);
8. architectural components of the design;
9. specific items of legislation referenced; and
10. indications of the need for extended evaluations (*e.g.*, further surveys, interviews, *etc.*).

The first four metrics were selected to measure the thoroughness of the analysis performed by the participants. The next four metrics measure the complexity of the resulting design. Finally, the last two metrics indicate references to external resources that had become necessary during the design process (*i.e.*, expressing the need to ask stakeholders for their opinion, reference legislation, *etc.*).

I counted the occurrence of each type of metric by classifying each statement or paragraph in the written reports. Guidance provided to the participants suggested a specific organization of their reports. However, only groups 2 and 3 loosely followed these suggestions. For this reason, the identification of countable occurrences of the analysis elements is not as rigorous as would be desirable. In many cases, elements were not explicit and had to be interpreted (see Table 5.1). In all three groups' reports, the report size (in number of paragraphs) is roughly proportional to the sum of all analysis elements.

The numbers in the table should be taken at face value and not compared across columns because they are the result of different analysis processes without any control on the amount of time used in the analysis. Also, these bare numbers do not indicate whether the identified analysis elements were pertinent and correct in the context of the specific analysis. To control this variable, I further examined each design choice made by the three groups to assess whether it had a strong impact on stakeholder privacy or security. The Reference columns provide numbers about the analysis performed by me.

5.1.4 Discussion

5.1.4.1 Usability

All three groups provided strong evidence of having understood the method's core concepts well enough to use the method or to make a justified decision not to use it. Group 1 did not use the design method, claiming that the existence of very similar commercial applications voided the need for applying a detailed design method. Both group members had a technical background and started the analysis from a feasibility assessment. They based their analysis on the comparison with two other similar applications. The comparison process, in their words, "jumpstarted" the design process and "gave a feel for what's possible."

Group 2 did use the design method but skipped the first phase (which requires balancing application usefulness with stakeholder privacy concerns), because these "requirements were already given" and they "did not feel necessary to justify that the application was useful." The existence of similar services on the market might have influenced this assessment.

Group 3 stated that they applied an iterative design process to discover design issues and decide upon them, as suggested by the proportionality method. The other two groups used a top-down process, in which broad architectural decisions were followed by detailed design.

Table 5.1: Deliverables Coverage At a Glance.

	Group 1	Group 2	Reference	Group 3	Reference
Application	Person Finder	Person Finder	Person Finder	Video Recording	Video Recording
Used Method	No	Yes	Yes	Yes	No
Analysis Elements					
Threats	0	3	3	13	5
Scenarios	0	3	0	0	0
Comparisons with Similar Apps	2	0	2	2	7
Stakeholders	(1)[40]	2	3	7	5
Requirements	12	5	5	9	12
Design Choices	8	11	11	15	13
Design Choices relevant to privacy / security	6	6	11	13	13
Open Design Issues	4	6	2	7	2
Architectural Components	4	4	1	5	NA[41]
Legislation	2	4	2	2	3
Extended Evaluation	0	0	3	3	0
TOTAL	33	38	31	63	47
Report Size[42]	98	102	106	197	145

[40] The number of stakeholders was not indicated explicitly.

[41] The reference design of the video recording application did not include an architectural description of the application.

[42] Expressed in number of paragraphs.

5.1.4.2 Usefulness

The groups using the design method provided evidence of engaging in more elaborate—and more time-consuming—evaluation of alternative design options which did not rely much on the critique of existing applications (see Table 5.1). Group 1 concentrated their analysis on the user interface of the application, specifying its design (hence the high value of the Requirements variable). The same group did not identify as many threats to stakeholders' privacy.

All participants who used the design method agreed that the application of the method had not increased the design time by itself, but they also indicated that they were encouraged to explore more design alternatives, and with greater depth, which required increased effort and time. Group participants that used the method commented in the interviews that their designs were more thorough because of method use than they otherwise would have been. This claim was reflected in the completeness of the deliverables written by the three groups. The group that did not use the method explored only one technological solution, primarily basing their design on a comparison with, and enhancement of, similar existing services, whereas the groups that used the design method generated comparably more detailed designs. The groups that used the design method identified a higher number of design issues (summing open design issues and design choices) than the group that did not.

One member who used the design method stated that "the hard part was playing both roles [involved in the balancing of stakeholder needs]." The balancing of cost-effectiveness, usefulness and privacy was also cited by another participant as a challenging, but useful exercise. In particular, the participant indicated that this process helped him in reaching decisions among alternative design options with privacy implications.

Finally, one group indicated that initially the application of the method had seemed "silly and redundant" but that eventually, the output of the analysis process, especially the documented evaluation of several alternative technical solutions, had been very useful as a *communication tool*. This group had talked about their design with potential stakeholders and had found that the design output had been useful to justify and describe a particular solution in that context. Participants in one group commented that the design method would be most appropriate for exploratory applications, and less so for established technologies.

5.1.4.3 Inter-Designer Stability

I did not observe sufficient evidence to support the thesis regarding the similarity of the participants' analyses to the reference analyses (see Table 5.2). Two groups, including the group that did not use the method, produced results that were quite different from the reference analysis (*i.e.*, there was little overlap between the design choices made by the participants *vs.* those made by the experts), whereas the third group produced a design similar to the reference design (there was higher degree of overlap). This might also be a function of the available literature, of the type of application at hand and of its description. Given these results, I skipped this analysis in the follow-up study.

Table 5.2: Overlap of Participants' Design With Experts' Design.

	Group 1	**Group 2**	**Expert**	**Group 3**	**Expert**
Design Choices relevant to privacy / security	6	8	11	13	13
Overlap with Expert[43]	21%	27%	N/A	53%	N/A

[43] Calculated as: *OC / TC* where *OC = number of choices on overlapping issues*; *TC = total number of unique choices* (group + expert).

5.1.5 Conclusions

Although it is not possible to infer strong quantitative conclusions from just three sources of qualitative design process data, this study encouragingly suggests that the proportionality method is usable for its intended purpose. Based on participants' comments and evaluation of the deliverables, I can make the following tentative observations:

- the method may be particularly fit for exploratory or novel applications that lack prior deployment history;
- the method may be most useful in cases of multiple stakeholders with diverging interests;
- the method may encourage designers in evaluating a larger number of design alternatives;
- the method added little overhead to the design process; and
- the end product of applying the method was useful to convince others about the validity of the design choices made (it contained a stronger rationale).

I did not gather sufficient evidence to support my second thesis, that the design process can produce repeatable outcomes across expert and non-expert designers.

5.2 The Design Method Evaluation Study

The pilot study provided some initial hints regarding the usefulness and usability of the proportionality method, but not enough quantitative evidence demonstrating its performance *vis-à-vis* other design methods or current best practice. Furthermore, the study suffered from an insufficient control of important independent variables, such as prior experience. For this reason, I conducted a follow-up design method evaluation study involving 48 participants.

This second study benefited from the experience gained from the pilot study. Specifically, the pilot study allowed me to test a design method evaluation process; the quantitative metrics developed for the analysis of the design products were employed with some modifications in this study; and experience from the interviews in the pilot study helped define the question set for the semi-structured interviews in this study.

5.2.1 Overview and Hypothesis

The purpose of the design method evaluation study was to measure the effectiveness of three methods for analyzing and solving privacy and security issues in ubiquitous computing applications. The students from two sections of the *Introduction to HCI* class at the College of Computing of Georgia Institute of Technology were asked to design a ubiquitous computing application with known privacy and security issues. The students were assigned to one of three conditions (one for each of design methods) and one control condition in a between-subjects experimental design. The four conditions were:

- Bellotti and Sellen’s feedback and control privacy framework [31] (henceforth called “Feedback / Control”);
- Hong *et al.*’s risk analysis for ubicomp privacy [92] (“Risk Analysis”);
- the proportionality method (“Proportionality”); and
- the control group used Design Rationale (“Design Rationale”) [124].

Bellotti and Sellen’s framework was chosen for comparison because it is, to my knowledge, the first design method proposed in the ubicomp community specifically for addressing privacy issues. It is a refinement of QOC (Questions, Options, Criteria), that suggests predefined questions and criteria (outlined in Table 3.1). Bellotti and Sellen’s framework was also used as a reference in other similar studies (*e.g.*, by Jensen [108], who compared it with a goal-driven analysis technique). Hong *et al.* proposed applying risk analysis and risk management to the design of ubicomp applications with privacy concerns. Their technique was selected for comparison because risk analysis is one of the prime analytic tools in IT security, but its effectiveness has not yet been evaluated in the specific context of ubiquitous computing.[44] The third group employed the proportionality method described in Chapter 4. The control group did not use any privacy- or security-specific method, and was instead instructed to use Design Rationale by MacLean *et al.* [124], a QOC requirements analysis and documentation technique well-known in the RE and HCI fields. Like Bellotti and Sellen's framework, Design Rationale proposes a QOC analysis, but unlike that framework, it does not suggest any specific question or criteria for privacy or the ubicomp domain.

The participants were asked to design an application similar to Microsoft's SenseCam [75],[45] using one of the four techniques. The design task was given as a week-long homework assignment. The performance of the design methods was assessed both using quantitative metrics (*e.g.*, number of privacy/security issues discovered and number of design choices made by each participant, time required to perform analysis) and qualitative analysis (*e.g.*, judgment on the quality of designs by independent reviewers, type of issues addressed).

The setup of this study is intended to shed light on the following questions: 1) whether any one design method is more effective than the others according to some performance metric; and 2) what are the qualitative differences across methods. Regarding the first question, my null hypothesis was that all four conditions are equivalent, in terms

[44] One problem of applying risk analysis in the ubicomp domain is that risk analysis (especially quantitative risk analysis) assumes that the analyst has a great deal of knowledge about security risks and their impact on stakeholders. Such knowledge is by definition difficult to acquire in the ubicomp domain.

[45] SenseCam is a pack-of-cards sized wearable camera that automatically captures images and stores them in its memory. It can be worn as a pendant hanging on the chest of the user. Events, such as time, movement, light level and temperature may trigger the capture of new information. For example, when the user walks into a room, a light change transition can be detected and an image is captured with a wide-angle lens. Accelerometer data is used to reduce blurred images caused by camera motion, which is an essential feature of any truly wearable camera.

of qualitative and quantitative metrics. I hypothesized that at least one of the three methods will provide better performance, in terms of design issues identified and a quality assessment by expert reviewers, than the control condition. Regarding the second question, the null hypothesis was that there would be no qualitative difference between the output designs in the four conditions in terms of the type of privacy and security issues identified. The hypothesis was that the type of questions probed by each method would qualitatively influence the type of designs issues addressed.

5.2.2 Experimental Procedure

The homework was part of the class syllabus, and every student had to perform it for class credit. Participation in this study was however voluntary, and 51 students volunteered to participate (out of approximately 65 enrolled students). Three participants later exited the study, because they were unable to complete the assignment and for other reasons, resulting in *N = 48*. The number of participants was deemed sufficient, during planning, to produce statistically significant quantitative results. However, the unexpectedly high variance of the results prevented obtaining statistically significant results in many cases.

Students who chose to participate agreed to be assigned to one of the four conditions and gave us permission to review their designs, their quiz grades and their course grades. Students choosing not to participate were given the option to attend any one of the four lectures and perform the homework according to that lecture.

The proportionality design method targets HCI designers without a specific training in security or privacy issues. The participants of this study (graduate students in a design course) were selected to represent a population of designers with low to moderate professional experience (see Figure 5.4). The demographics of the participants match the goals of the study because the design methods aim at aiding designers who operate in a field (ubiquitous computing) that does not have an established base of design knowledge.

The students from both sections in the study were randomly assigned to one of four groups, with the following condition. The *Introduction to HCI* class at this Institute requires students to work in groups of four on a semester-long project. Students within these groups have extensive contact with each other. Recognizing that students within the same semester project group would have more opportunities to communicate about the homework, I assigned them to different experimental conditions in the effort to discourage them from influencing each other. This task was facilitated due to the fact that projects groups are usually composed of 4 students, as many as the conditions in this study.

5.2.2.1 Enrollment

At the beginning of the semester, students were given a information notice about the study, per Institutional Review Board (IRB) requirements. Students enrolled in the study two weeks prior to the design method lecture in class. To increase the likelihood of participation, I highlighted the educational aspects of the study. Contact information and consent forms were collected from all participants during enrollment. At this point, students also completed a demographic survey, including design and domain experience (to control for prior experience), degree program, year in program, and Harris-Westin privacy preferences [149].

5.2.2.2 Lectures

Each condition received a distinct lecture on the assigned design method. The lectures were all similar except for the design method presented. They all introduced the issues of privacy and security in ubicomp, and the specific design method. The lectures also included a sample application of the design method to the Personal Audio Loop, and a short description of the homework task. The same instructor gave all four lectures.

Students were given paper copies of the respective design method reference paper, and the lecture's slides. A digital link to the SenseCam CARPE '04 paper [75] was also given to participants, along with other relevant bibliographic references, listed in the design brief in Appendix B. This “facilitation material” was necessary because students did not have enough time to perform bibliographic research on the design and I wanted to provide a consistent amount of basic knowledge about the application domain. Students were asked to cite any other sources they used.

5.2.2.3 Exercise

At the end of the lecture, students were given an application brief that asked them to design an application, based on the SenseCam, that would support non-verbal children and their parents to communicate about the child’s daily activities at school. The SenseCam technology and this application represent a particularly good case study because there are still few publications about the technology and this scenario presents multiple, diverging, stakeholders. On the other hand, the application and technology are conceptually small enough that design was manageable within the given time constraints. Participants were instructed to focus on the privacy and security aspects of the design, and given freedom to alter the operating parameters of the SenseCam as deemed necessary. An excerpt of the design brief follows:

> *Non-verbal children (such as some children with disorders in the Autism spectrum) may be unable to recount daily activities at school to their parents when they get home. This reduces parents’ knowledge of the children’s activity when out of the home, and of their mood or feelings. If the children carried a SenseCam, their parents may be able to better reconstruct the child’s activity independently from the reporting of the teachers or caregivers in school. This improved knowledge, in the form of an automatically-authored daily journal, may improve the parent’s understanding of the child’s feelings and thus his or her response to their needs or con-*

> *tingent behavior. […] You are asked to design a system that would support the application described above, especially focusing on privacy and security concerns. You are free to define the parameters and the design of the SenseCam device and of the other components of the system in any way you deem fit for achieving the goals of the application, including the fact that it is wearable, how pictures are taken, or additional sensing such as audio, video or other.*

The complete text of the design brief and a list of references provided to participants are reported in Appendix B. The choice of the design assignment is crucial in this kind of study and deserves an explanation. This brief strikes a middle ground between two options represented by the use of the design methods for summative critique as opposed to formative design (see the discussion in Chapter 3). The former would suggest to evaluate the design methods by providing students with a certain number of designs and have them critique these designs using one of the four design methods. According to the latter alternative, students would have developed designs from nothing, employing the design methods as formative tools for making reasoned design decisions. I decided to settle on a mixed evaluation / design exercise because: 1) the proponents of the design methods do not specify whether they are intended for summative or formative use; 2) the timeframe given to students would not have allowed a deep enough analysis had they started from nothing; and 3) I wanted to constrain the design space somewhat to achieve a certain uniformity and comparability between design outputs. As a result, I asked the participants to evaluate a high-level design, given by us, by identifying risks or privacy issues, and design eventual changes and the detailed design features of the application based on the conclusions of their analyses.

I asked for a final deliverable of 1600–2400 words (4–6 pages), suggesting that it would take 6–8 hours of time to perform the assignment over one week. The reward structure was based on the comprehensiveness of the design document and students were informed of this in class. I chose not to evaluate time performance (*e.g.*, counting the number of issues found in a fixed period of time) because I was interested in students reflecting on the designs, coming up with solutions over a reasonable amount of time—striving to mimic how actual design tasks are accomplished—rather than engaging them in a design speed contest.

Participants were asked to follow closely the design method they had been assigned to and to explain any deviations from the assigned method (*e.g.*, if they felt that there were important issues that would not arise from the application of the method). Participants were asked to keep track of how much time they spent doing the assignment using a simple form, similar to those used in techniques like the Personal Software Process [94]. They were asked to track time spent on researching and gathering information separately from the time spent on designing and writing up the assignment. It was stressed that participants would not be evaluated on this information. Time-tracking allowed me to control for performance/cost variables across conditions. Students received two reminder emails prompting them to keep track of the time spent on the assignment, and to remind them to bring the sheet to class with the assignment.

When submitting the assignment, students were asked to complete a post-study questionnaire with questions about the use of bibliographic and other sources (individuals with whom they spoke about the assignment, reference material, *etc.*), Likert questions about the experience of using the design method (effort to understand, effort to apply, *etc.*), and some other procedural information (*e.g.*, willingness to participate in an interview). At this point, students also completed an anonymous “satisfaction” survey that gave them the opportunity to express their opinions on the design method and on the study. Assignments were graded by the two Teaching Assistants (TA) in the class (each TA graded half of the assignments, distributed pseudo-randomly across conditions). Additionally, each TA *evaluated* all assignments on novelty, comprehensiveness and clarity.

Both TAs were PhD students with experience in HCI at our institution (verified using an experience questionnaire similar to that used for participants). To get a sense of the reliability of these evaluations, I measured inter-rater consistency.

An adherence score was also computed for each homework. The adherence score is a value between 0 and 1 that indicates how closely the participant applied the given design method. It is computed as the proportion of design steps that the participant followed in the assignment, relative to the design steps described in the reference paper (see Appendix B for a formal definition of the design steps).

5.2.2.4 Quiz

After submitting the assignment, students completed in-class quizzes to verify their understanding of the design method. This test was necessary to control for potential unequal understanding of the design method. Individualized quizzes for students in the four groups were provided. The quiz also provided class credit. Summary analysis of the quiz grades indicates that the majority of participants demonstrated having well understood the design method. Graded quizzes were returned to the students. A sample quiz is found in Appendix B.

5.2.2.5 Interviews

Interviews were held before the end of the semester, 2–3 weeks after the assignments were turned in. Interview participants received token retribution of USD10 to motivate them to participate, given their busy end-of-semester schedules. A selection of participants was invited via email to take part in a short semi-structured interview (lasting 15–20 minutes). I attempted to select, from each experimental condition, one participant who achieved a high evaluation score by the TAs in the design and one or two who achieved a low score. In total, this would have provided 8–12 interview participants. Seven participants were actually interviewed, due to the impossibility to schedule all planned interviews. In the interview, participants were asked subjective questions about the application of the design method, including their assessment of the quality of the resulting designs, the effort required, and the effects of using the design methods.

5.2.2.6 Collected Metrics

Several metrics were collected about each participant and his or her design (see Table 5.3). In the table, each metric is named and explained. The source of the metric is also indicated in the second column. The source indicates who has quantified the value of the metric. Finally, each metric is given a variable name if it was used in the quantitative analysis. It should be noted that the choice of metrics is necessarily based on considerations that are arbitrary to a certain degree. The first seven metrics refer to a coding of the design deliverables. Each deliverable was analyzed and significant assertions, falling into one of the seven categories were flagged as such. Metrics T and C are particularly important. T indicates the number of security / privacy issues (or "threats") identified in the deliverable (*e.g.*, "the user may lose the SenseCam device"). C indicates the design choices or requirements (*e.g.*, "Access to the pictures taken by SenseCam should be password-protected"). The idea of using the number of identified security / privacy issues derives in part from work on Heuristic Evaluation, in which "usability issues" are identified, prioritized and counted to show the effectiveness of discount usability techniques [135]. Furthermore, the identification of security / privacy issues is common in risk analysis and management in the security community. Finally, the identification of security issues is also common in security requirements engineering models such as the Common Criteria [105]. In the Common Criteria, *security threats* (*i.e.*, issues) must be addressed by *security objectives*, reflecting security RE practice. Security objectives relate to the *design choices* measured in this study (variable C). Anecdotal evidence from the deliverables indicates that, in many cases, design choices are made to address security issues, with a weak correlation between T and C: $r(T,C) = 0.26, p < 0.05$ one-tailed.

Table 5.3: Metric Collected for each Participant.

Metric	**Source**	**Explanation**	**Variable**
Number of privacy/ security issues	Researcher	Number of Identified privacy/security issues or threats (*e.g.*, “the user may loose the SenseCam device”). These issues have been cataloged and grouped in Table 5.10.	T
Number of usage scenarios	Researcher	Number of usage scenarios. This metric was counted because scenario-based requirements analysis has been proposed as a requirements elicitation method. I counted scenarios that were presented as a short narrative, and not threat scenarios.	N
Number of comparisons with existing, similar applications	Researcher	Comparison with existing applications; for example, comparisons with a digital camera, or surveillance in schools. This metric is included because designing a novel application is often done *by analogy*, looking at other, similar existing applications for reference.	X
Number of identified stakeholders	Researcher	The number of identified stakeholders (*e.g.*, the parents, the child, *etc.*). Note that none of the four methods provides specific help in identifying stakeholders. Stakeholder analysis is however a fundamental component of multilateral security and was requested as part of the assignment.	S
Number of stated design choices	Researcher	Number of stated design decisions or requirements (*e.g.*, “Access to the pictures taken by SenseCam should be password-protected”). This metric is a proxy of the design complexity or depth. Not all design choices are at the same level of complexity. Also, participants did not really have the chance of *solving* design issues with specific design choices because they lacked the ability to evaluate their choices—so this metric counts as “proposed design choices.”	C

Table 5.3: Metric Collected for each Participant. (Continued.)

Metric	**Source**	**Explanation**	**Variable**
Number of open questions	Researcher	Questions that were raised by the participants but no conclusion was reached, pending more information or the verification of some other hypothesis (*e.g.*, specific items of legislation referenced, further surveys, interviews, *etc.*).	O
Number of value propositions	Researcher	Value propositions for the application, *i.e.*, statements about the usefulness of the application . This metric is important because value propositions are used in some of the methods to justify privacy-invasive choices (*e.g.*, in the Proportionality method and in Risk Analysis).	V
Deliverable Size	Researcher	Computed as T + N + X + S + C + O + V [46]	Z
Adherence score	Researcher	Estimate of how accurately the participants followed the design method process. The formal definition is provided in Appendix B.	A
Novelty Comprehensiveness Clarity	Evaluators	Design quality of each report as evaluated by independent reviewers. The Quality metric Q is the average of the 3 scores given by each evaluator. All these scores are based on the scale (0: not novel/comprehensive/clear – 6: very novel/comprehensive/clear).	EN_e[47] EC_e EL_e Q
Homework grade	Evaluators	Assigned by the TA to the design deliverable.	G
Quiz grades	Researcher	Assigned by researcher.	QU

[46] The pilot study suggests that this value is well correlated with the size of the design deliverable.

[47] The notation EN_e indicates the value of the variable EN computed by evaluator *e*.

Table 5.3: Metric Collected for each Participant. (Continued.)

Metric	**Source**	**Explanation**	**Variable**
Demographic information	Participant	Degree program, year in program, *etc.*	
Design experience metric	Participant	IT development experience, RE experience, Ubicomp experience, experience with surveillance and C&A systems. *EX = Σ (years of commercial or research experience in these fields) + 1/3 Σ (number of courses on these topics)*	EX
Design method's Usefulness Easy to apply Would use again in the future Impact on time Impact on quality	Participant	Subjective scores of the usefulness and usability of the design method (scale 0: strongly disagree…6: strongly agree).	
GRE	Participant	General GRE score.	GRE
Privacy attitude before study Privacy attitude after study	Participant	We administered the Harris-Westin privacy segmentation questionnaire both before and after the study. This metric was developed in the context of data protection concerns towards commercial organizations and classifies individuals in one of three categories: privacy pragmatist, fundamentalist and unconcerned.	
Time spent researching Time spent designing and writing assignment	Participant	The time employed for the design exercise by the participants. TR indicates the time spent researching and reading. TD is the time spent designing and writing up the assignment. TT is the total time. *TT = TR + TD*	TR TD TT

Table 5.4: Controlled Variables.

Variable	**Control(s)**
Different presentations of the assignment or design method in the four groups.	Control over presentation: same presenter for all four conditions; prepared, uniform slides across conditions.
Presenter might have vested interest in one method.	Have presentations made by an "independent" presenter.[48]
Influence of external people.	Ask at the end of the study if there were exchanges with other individuals.
Individual students collaborating, especially within project groups.	Ask students not to collaborate, verify for similar designs (typical homework practice). Assign students in same project groups to different conditions.
Participants' prior knowledge.	Control with demographic survey.
Availability of reference literature.	Provide basic literature to everybody. Ask to explicitly reference other sources.
Different student proficiency in two sections.	Controlled by randomizing across sections.

[48] The lectures were given by Gregory Abowd, who is co-author of the Proportionality paper and may thus be biased in the delivery of the lectures. He is also a very experienced HCI researcher and was available to teaching the lectures in the tight schedule. In my opinion, he delivered unbiased lectures—differences across conditions, if any, were caused from his increasing proficiency at delivering the common parts of the lecture over time.

The other variables are useful to quantify secondary trends worthy of note and to provide a complete synthetic picture of the design deliverables. In fact, coding each paragraph of the design deliverables as one of T, C, N, X, O, S, V, leaves very few paragraphs not coded.

As a final note, the process of classifying elements of a written deliverable into these 7 categories is necessarily imprecise, and the resulting numbers should be taken with caution. Having multiple raters perform this task would have provided a higher degree of reliability, but the cost associated with this analysis was incompatible with the timeline and budget of this project. The same observation holds for the categorization of the type of security / privacy issues identified by the participants and listed in Table 5.10.

5.2.2.7 Controlled Variables

Several important variables were intentionally controlled in the design of this study (see Table 5.4). As mentioned above, design is a complex activity and good designs may originate because of many different reasons. Controlling as many external influences as possible is mandatory for obtaining relevant data.

5.2.3 Demographics

The study involved students from both sections of the CS/PSYC 6750 *Introduction to HCI* class at this institution, *N = 48*. Table 5.5 lists participant subdivision across the four conditions, and the reference paper given to each participant describing the respective design method. It was not possible to divide participants equally across conditions because of scheduling constraints (to accommodate study requirements some participants were asked to attend a lecture outside of their normal class hours and this caused conflicts).

Table 5.5: Four Conditions of Participants in Study.

Condition	**Paper provided to participants** **(in parentheses the case study discussed in paper)**	**Participants**
Feedback / Control	Bellotti and Sellen's 1993 ECSCW paper [31] (video awareness system as case study)	$N_1 = 11$
Risk Analysis	Hong *et al.*'s 2004 DIS paper [92] (person finder case study)	$N_2 = 12$
Proportionality	Iachello and Abowd's 2004 CHI paper [97] (PAL case study)	$N_3 = 13$
Design Rationale (Control group)	MacLean *et al.*'s 1989 CHI paper [124] and HCI textbook [56] (examples from WIMP UI)	$N_C = 12$

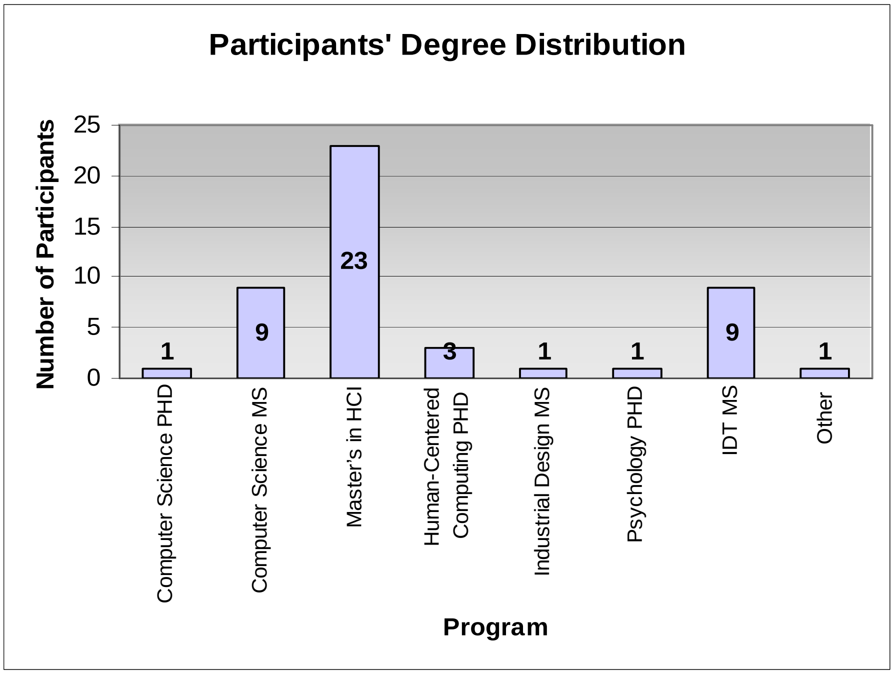


Figure 5.1: Distribution of Participants' Degree.

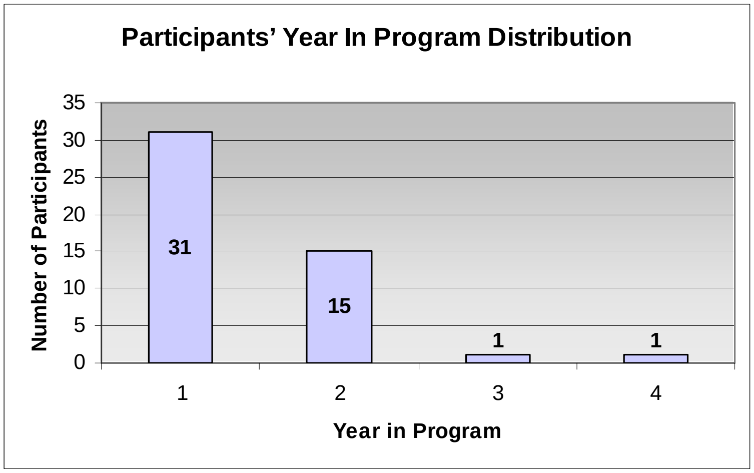


Figure 5.2: Distribution of Participants' Year in Program.

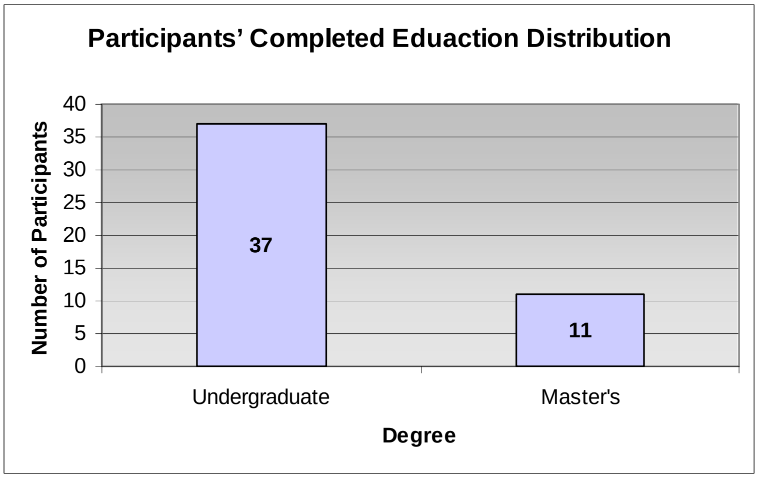


Figure 5.3: Distribution of Participants' Completed Education.

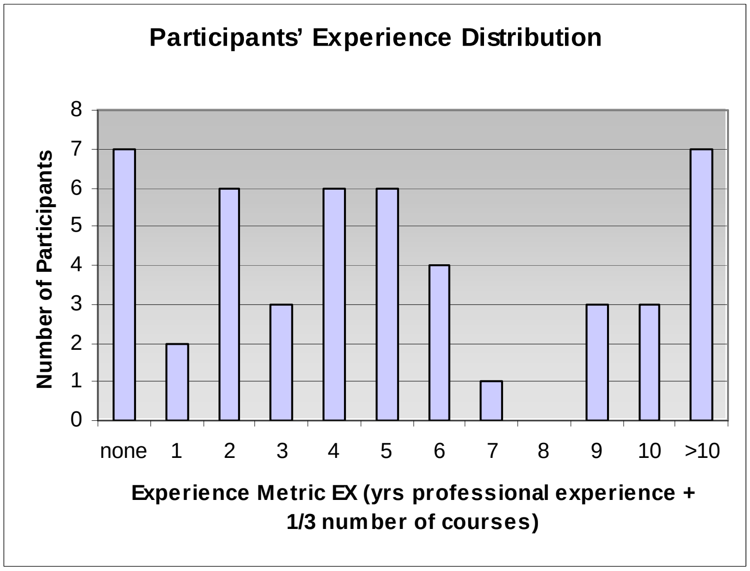


Figure 5.4: Participants' Experience Distribution.

5.2.3.1 Degree Program and Education of Participants

Basic demographic information about the participants' degree program, year in program and completed education was collected (see Figure 5.1 – Figure 5.3). The majority of participants were master students, in the Computer Science, HCI and IDT degree tracks, which is consistent with their level of completed education (predominantly undergraduate degrees) and their program year (predominantly, 1st and 2nd year).

5.2.3.2 Experience of Participants

The distribution of the participants' experience metric EX (defined in Table 5.3) shows two groups: namely experienced ($EX > 8$) and inexperienced ($EX < 8$) participants with overall $mean = 5.1$, $\sigma = 4.8$ (see Figure 5.4). Table 5.6 shows the same variable numerically and divided by condition. The overall variance of this variable is very high (comparable to the absolute value) in all four conditions, indicating that the recruitment process yielded a mix of students without significant professional experience and of participants returning to get an advanced degree after working in commercial organizations. An ANOVA test showed that there are no significant differences of experience across conditions, ensuring that the performance differences across conditions coming up later in the analysis do not stem from experience differences of the participants in those conditions.

Very few participants had good knowledge of requirements engineering frameworks and laws prior to the study (see Table 5.7, which shows the number of participants who claimed to have worked with some Requirements Engineering frameworks of interest or with specific items of privacy-related legislation). The only exceptions are Design Rationale, which was explained in a previous lecture in the same course, and HIPAA. However, knowledge of HIPAA did not correlate significantly with differences in the mean number of identified privacy/security issues T.

Table 5.6: Experience of Participants.

Condition	**Mean**	**N**	**σ**
Feedback / Control	4.1	11	3.0
Risk Analysis	5.4	12	4.2
Proportionality	5.6	13	5.4
Design Rationale	5.3	12	6.4
Total	5.1	48	4.8

Table 5.7: Participants' Experience with RE Frameworks and Legislation.

"Please list all requirements engineering frameworks and methodologies (or legislation) you had experience with (*i.e.*, worked with or researched on)." [Questions 7 and 10 form DS-Q1]	**Number of Participants who answered yes (N=48)**
Design Rationale	17
Win-Win requirements analysis	1
Risk Analysis frameworks	5
Other	1
Electronic Communications Privacy Act (ECPA)	1
Health Insurance Portability and Accountability Act (HIPAA)	10
Family Educational Rights and Privacy Act (FERPA)	3
Gramm-Leach-Bliley Act (GLBA)	0
Privacy Act of 1974	2
Court Rulings	1

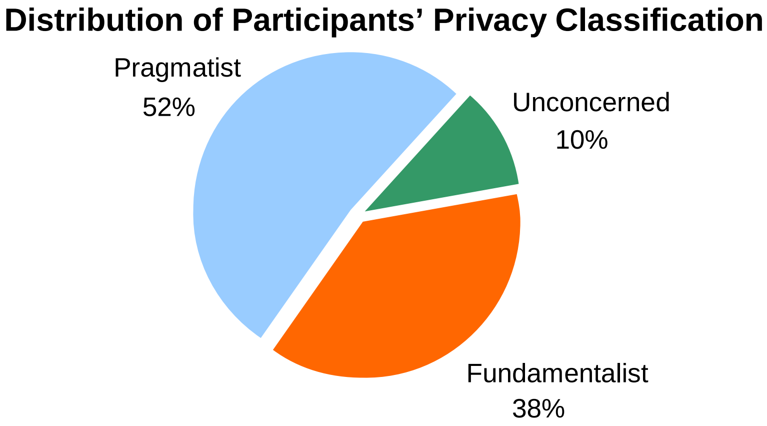


Figure 5.5: Privacy Classification of Participants (Harris-Westin Survey).

5.2.3.3 Privacy Preferences

The participants represent a typical population in relation to their general attitudes towards privacy, as measured by the Harris-Westin privacy segmentation (Figure 5.5).[49] I measured this classification because it is a widely employed privacy classification, and I desired to verify that the participants belonged to a 'normal' sample with regards to data protection issues. However, I do not relate privacy classification with the design output of the participant, because this classification, targeted at consumers, is in my opinion inappropriate for describing designers and their activity.

5.2.4 Quantitative Analysis

In this section, I present a subset of all the quantitative analyses that were performed on the data, limited to those that are useful for stating some claim in the discussion below. Each analysis is presented within a different sub-section.

[49] Based on recent surveys, roughly 60% of individuals fall in the pragmatist category, roughly 30% are fundamentalists and the rest privacy unconcerned [179].

Table 5.8: Time To Complete Assignment.

Time Employed to Perform Assignment (TT = TR + TD)	**Control / Feedback**	**Risk Analysis**	**Propor-tionality**	**Design Rationale**	**Total**
N (participants)	11	10	11	12	44[50]
TT Mean (hours)	9.89	10.37	9.08	10.34	9.92
σ (hours)	3.16	2.85	3.46	2.90	3.04
Minimum (hours)	4.00	5.50	3.83	6.50	3.83
Maximum (hours)	16.50	15.00	14.50	15.92	16.50

5.2.4.1 Time to Complete Assignment

Most participants took more time to complete the assignment than the 6–8 hours we had expected. Participants in the four conditions did not show significant differences in the amount of time necessary to complete the assignment (Table 5.8). Moreover, participants' comments on the post-questionnaire and in the anonymous feedback forms indicated that they felt that the assignment would have required more time to perform exhaustively. Table 5.8 provides statistics for TT. Time was allocated approx. ⅓ researching (TR) and ⅔ designing (TD) and writing up the report. Differences across conditions were not significant according to an ANOVA analysis.

5.2.4.2 Inter-rater Consistency

Recall that I used two independent evaluators to assess the designs' comprehensiveness (EC), clarity (EL) and novelty (EN) for each homework. There is good inter-

[50] I removed two outliers. Two additional participants did not return the timesheet.

rater consistency on all three metrics. This suggests that the quality metrics assessed by the evaluators are in fact reliable and interpreted in the same manner.

$$r(EN_1, EN_2) = 0.49,\ \ p = 0.001.^{51}$$

$$r(EC_1, EC_2) = 0.41,\ \ p = 0.004.$$

$$r(EL_1, EL_2) = 0.65,\ \ p < 0.001.$$

The design quality variable was defined as the average of all the evaluations given by the two evaluators:

$$Q = (EN_1 + EN_2 + EC_1 + EC_2 + EL_1 + EL_2) / 6.$$

The quality metric correlates to the grade assigned to the homeworks:

$$r(Q, G) = 0.59, p < 0.001.$$

This correlation suggests that comprehensiveness, clarity and novelty were reflective of an overall quality judgment expressed by the grade of the homework. Moreover, grades, although assessed by two separate evaluators, can be compared (each TA graded only half of the assignments to reduce their work, but evaluated all assignments on EC, EL and EN).

5.2.4.3 Comprehensiveness vs. Number of Issues Identified and Number of Design Choices

Comprehensiveness EC correlates weakly with deliverable size Z:

[51] *r(A,B)* indicates correlation between the variables A and B, over the whole sample set (N = 48) unless otherwise noted. Some samples are missing from some calculations because of missing data items, or because of eliminated outliers and this is noted where appropriate.

$$r(Z, (EC_1 + EC_2) / 2) = 0.329, p = 0.012.$$

This level of correlation suggests that longer assignments were not just ‘longer’, but were also judged to be more comprehensive by the evaluators.

The number of privacy / security issues T correlates significantly with comprehensiveness EC for evaluator 1 but not for evaluator 2. Moreover, average comprehensiveness is not significantly correlated with the number of identified privacy / security issues.

$$r(T, EC_1) = 0.29, p = 0.044.$$

$$r(T, EC_2) = -0.021, p = 0.889.$$

$$r(T, (EC_1 + EC_2)/2) = 0.071, p = 0.320, N = 46.$$

The number of design choices does not correlate to the comprehensiveness score given by single evaluators. However, the number of design choices C correlates weakly to the average comprehensiveness metric ($EC_1 + EC_2) /2$ provided by the evaluators:

$$r(C, EC_1) = 0.14, p = 0.325.$$

$$r(C, EC_2) = 0.275, p = 0.062.$$

$$r(C, (EC_1 + EC_2) / 2) = 0.261, p = 0.038, N = 47.$$

This level of correlation suggests that evaluator 1 was influenced more by analytic detail (T) in judging the design comprehensiveness, while the evaluator 2 was influenced more by design complexity (C). Overall, average comprehensiveness across evaluators is better correlated with design complexity than analytic detail.

5.2.4.4 Correlation of Grade and Quality with Number of Security / Privacy Issues Identified and Design Choices

There is weak significant correlation between the number of security and privacy issues identified by the participants and overall grade. Similarly, there is a weak significant correlation between the number of design choices and grade.

$$r(G, T) = 0.337, \; p = 0.010, N = 48.$$

$$r(G, C) = 0.307, p = 0.018, N = 47.$$

There is no correlation, however, between these two metrics and quality:

$$r(Q, T) = 0.070, p = 0.318, N = 48.$$

$$r(Q, C) = 0.118, p = 0.211, N = 48.$$

This absence of correlation, and the numbers reported above, suggest that the thoroughness, measured in terms of T and C, of the analysis and design may have influenced the overall sense of comprehensiveness, resulting in a marginally higher grade, but do not necessarily affect a “quality judgment.”

5.2.4.5 Correlation of Security / Privacy Issues Identified with Design Choices

The number of security / privacy issues correlates weakly with design choices:

$$r(T, C) = 0.258, p = 0.038, N = 48.$$

In many assignments, some of the design choices were stated in the beginning when providing general details about the application, and some were listed after the analysis of the security issues. Some of the latter design choices were taken to directly counter potential threats to security and privacy. This partial correlation may be a symptom of the latter type of design choices.

5.2.4.6 Correlation of Time Required to Complete Assignment with Number of Security / Privacy Issues Identified and Design Choices

Eliminating 4 participants,[52] there is significant correlation between the time needed to complete the assignment and the number of security / privacy issues identified.

$$TT = TR + TD$$

$$r(TT, T) = 0.334,\ p = 0.027,\ N = 44.$$

However, there is no correlation between this time and the complexity of the design (number of design choices). Even when eliminating 7 outliers, correlation is low and not significant:

$$r(TT, C) = 0.077,\ p = 0.632,\ N = 41.$$

These correlations suggest that identifying issues increased significantly the time spent on the assignment, while coming up with a more detailed and complex design did not. In general, one may doubt whether the design choices were made to respond to the identified issues, or participants were following their own design ideas, independently of the identified issues.

5.2.4.7 Correlation of Experience with Number of Identified Issues and Design Choices

Recall the experience metric defined above:

$$EX = \Sigma\,\textit{number of years of professional experience in relevant IT fields} +$$
$$1/3\ \Sigma\,\textit{number of courses in relevant IT fields}$$

[52] These excluded data points include one outlier that was more than 3 standard deviations from the mean and three not-reported values.

"Relevant IT fields" are: general IT development experience, RE experience, Ubicomp experience. The number of identified issues correlates weakly to the experience metric:

r(EX, T) = 0.270, p = 0.033, N = 47 (excludes the highest T value).

This observation is confirmed by interviews, and suggests that prior experience has an impact on the thoroughness of the analyses. There was no significant correlation between experience and number of design choices:

r(EX, C) = 0.150, p = 0.154, N = 48.

These results suggest that prior experience may have helped participants in identifying security and privacy issues (the analytic phase of the assignment), but not necessarily in specifying detailed designs.

5.2.4.8 Correlation of GRE Score with Number of Identified Issues and Design Choices

There is no significant correlation between GRE scores of participants and the number of identified issues or design choices. I did not collect GRE scores from all participants (either because participants had not taken the GRE exam, did not recall the score or did not want to disclose it), but this suggests that student proficiency, as measured by the GRE score, did not affect the deliverables. It should be noted that the admission process to the Institute produced a set of participants with very similar GRE scores. I did not use GPA scores for measuring proficiency, recognizing that most participants would be in their first year at Georgia Tech and would be coming from different undergraduate institutions, and would thus have incommensurable GPAs.

5.2.4.9 Descriptive Statistics of Relevant Metrics

Table 5.9 reports the descriptive statistics of some of the following metrics used in this quantitative analysis: T, C, N, X, S, O, V, Z, G, Q, A. These statistics are divided by condition, and report the mean and standard deviation of the variable (fuller statistics are reported in Appendix C). Numbers of particular interest are contained in shaded cells. Figure 5.6 and Figure 5.7 show the means of these variables in graphical form. These descriptive statistics are used in the analyses reported below. Some numbers in Table 5.9 are noteworthy, and are highlighted in a shaded cell. The mean adherence score in the Risk Analysis condition is lower than the others because few participants completed the risk management part of the process, in part due to time limitations and in part possibly due to the difficulty and low perceived utility of performing the semi-quantitative risk comparison. Similarly, many participants in the Proportionality condition did not complete the Adequacy phase. In contrast, participants using the two QOC methods managed to cover most of the process steps.

In general, participants included in the deliverables few scenarios, open-ended questions and comparisons with other applications. Only the Proportionality method explicitly suggests employing the latter design element. The number of value propositions (V) is particularly low in the Design Rationale condition. This difference may be due to the fact that in the other three conditions, the method process reminded participants to state at least one value proposition (Proportionality frames it in terms of ‘usefulness,’ the Feedback / Control framework talks about ‘purpose’ and Risk Analysis explicitly requires designers to state the ‘value proposition’ of the application).

5.2.4.10 Difference in Means: Security / Privacy Issues, Design Choices, Grade, Quality As a Function of Condition

In this section, I compare the difference in means of the variables reported in Table 5.9. It should be noted that at this point, the comparison is not intended to support a claim that any method is ‘better’ than the others for specific design performance goals. The statistics are provided and commented with reference to the individual design method, with the intent of discovering the effects of the structure of different methods on the final deliverable.

An ANOVA test was used to analyze the differences in the means of the variables of interest summarized above (identified issues T, design choices C, grade G and quality metric Q). Although the graphs reported below (Figure 5.6 and Figure 5.7) suggest that these variables present different means across conditions, in general, these differences are not significant (the full data of this analysis is provided in Appendix C), due to the high variances of the results (see Table 5.9).

Only the following differences are statistically significant ($p < 0.05$) and can be explained *post-hoc* by considering the structure of the four design methods.

Identified privacy/security issues (T), between conditions Feedback / Control and Risk Analysis (*mean difference = 3.43, p = 0.01*). Risk Analysis offers a large number of questions that the designers must answer, which are designed to identify risks (which translate to security and privacy issues), whereas in the Feedback / Control framework, the issues are, so to speak, inherent to the method and relate to those issues typically found in awareness and multimedia conferencing systems that led Bellotti and Sellen to write their paper. Perhaps Feedback / Control does not help to think ‘out of the box’ in terms of privacy and security issues for different kinds of applications.

Table 5.9: Descriptive Statistics of Relevant Metrics.

Condition		**Feedback / Control**	**Risk Analysis**	**Proportionality**	**Design Rationale**	**Total**
T Number of Identified Security/Privacy Issues	Mean	5.18**	7.83**	6.85	6.25	6.56
	Std. Dev.	3.31	3.24	2.34	1.66	2.78
C Number of Design Choices	Mean	10.64	9.33	10.08	8.42	9.60
	Std. Dev.	3.88	2.67	3.99	5.26	4.01
N Number of Scenarios	Mean	0.18	0.00	0.08	0.00	0.06
	Std. Dev.	0.40	0.00	0.28	0.00	0.24
X Number of Comparisons to Similar Apps	Mean	0.00	0.00	0.62	0.33	0.25
	Std. Dev.	0.00	0.00	0.77	0.89	0.64
S Number of Stakeholders	Mean	6.82	4.75	5.23	6.42	5.77
	Std. Dev.	3.09	1.60	1.17	2.84	2.36
O Number of Open-ended Issues	Mean	0.36**	0.25**	1.69**	0.83	0.81
	Std. Dev.	0.50	0.62	1.25	1.59	1.21
V Number of Value Propositions	Mean	1.36	2.00**	1.92	0.75**	1.52
	Std. Dev.	0.81	1.28	1.55	0.62	1.22
Z Size of the Deliverable	Mean	24.55	24.17	26.46	23.00	24.58
	Std. Dev.	7.19	4.86	7.13	7.07	6.55
G Grade (1–10)	Mean	8.77	8.21	8.65	8.46	8.52
	Std. Dev.	1.54	1.03	0.69	0.72	1.02
Q Quality (0–6)	Mean	4.24**	3.21**	3.96	3.83	3.81
	Std. Dev.	0.99	0.79	0.95	0.93	0.96
A Adherence (0.0–1.0)	Mean	0.80	0.66	0.71	0.93	0.78
	Std. Dev.	0.37	0.30	0.21	0.13	0.28

** Differences in means are significant $p < 0.05$.

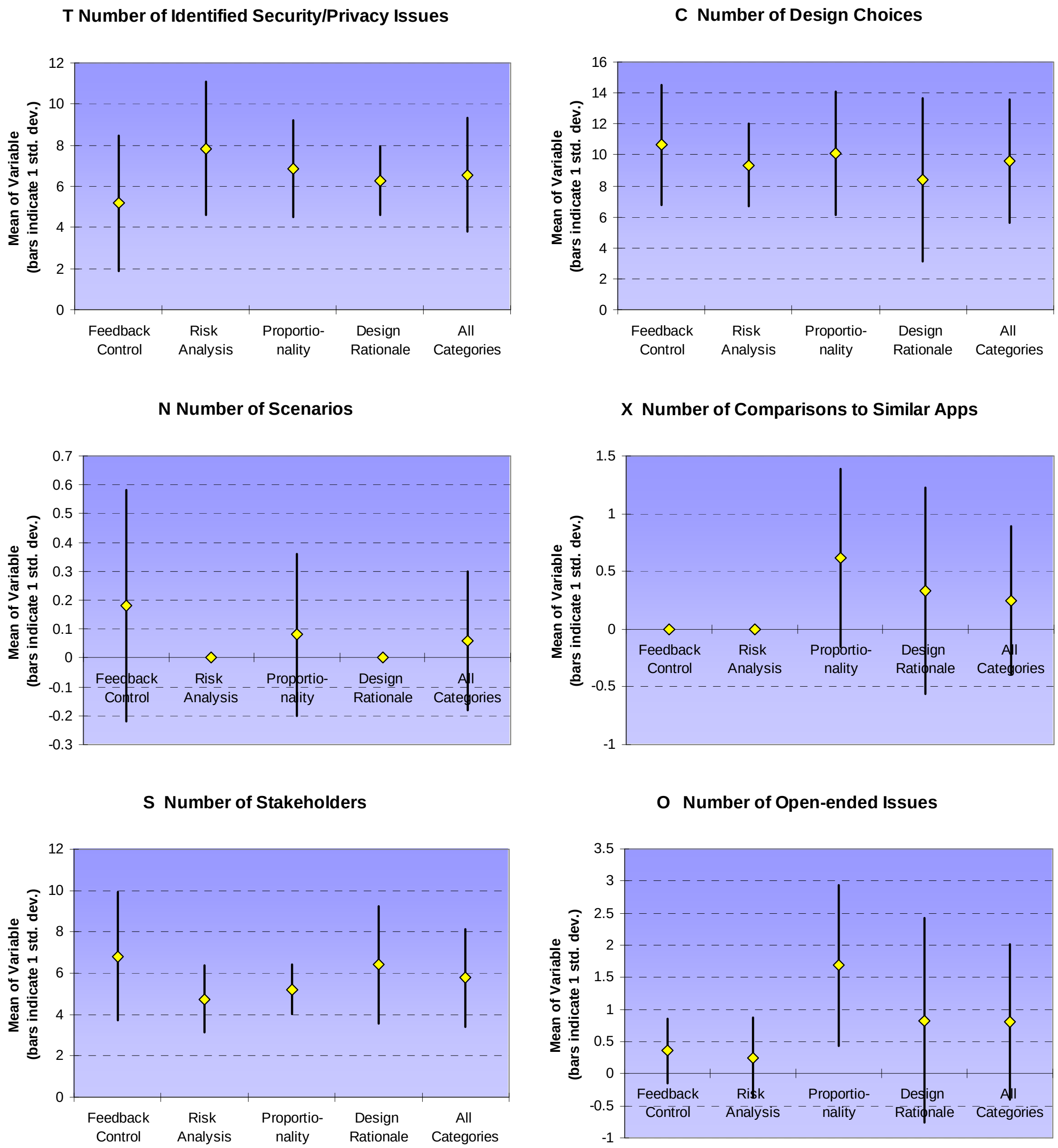


Figure 5.6: Graphs of Means of Variables T, C, N, X, S, O across conditions.

Diamonds indicate mean; vertical bars indicate ±1 standard deviation.

Significant differences: Identified privacy/security issues (T), between conditions Feedback / Control and Risk Analysis;

Number of open-ended design issues (O), between conditions Proportionality and Feedback / Control and Risk Analysis and Feedback / Control.

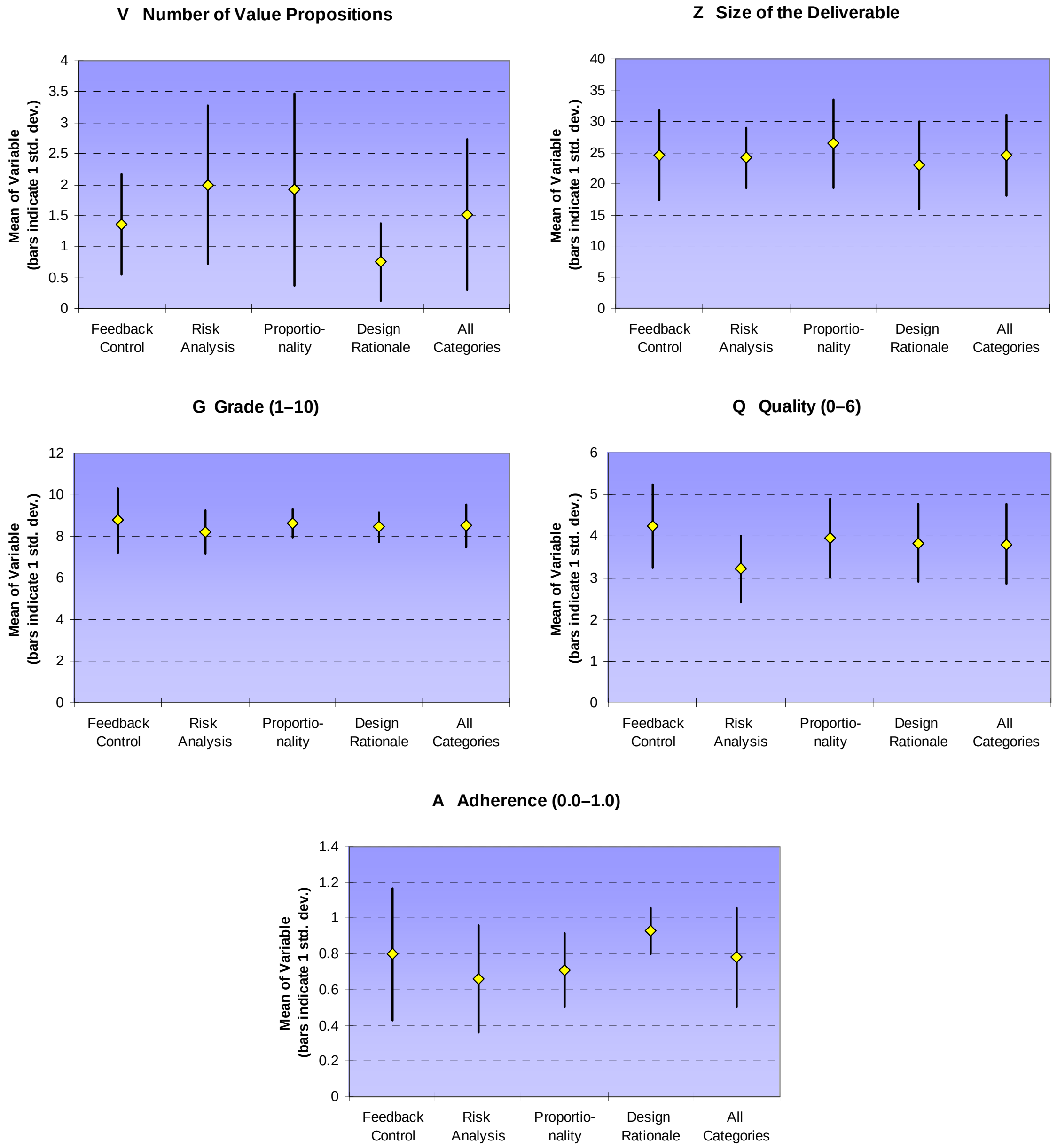


Figure 5.7: Graphs of Means of V, Z, G, Q, A.

Diamonds indicate mean; vertical bars indicate ±1 standard deviation.

Significant differences: Number of value propositions (V), between conditions Risk Analysis and Design Rationale;

Quality metric (Q) between conditions Feedback / Control and Risk Analysis.

Number of open-ended design issues (O), between conditions Proportionality and Risk Analysis (*mean difference 1.44 (p = 0.011)* and between conditions Proportionality and Feedback / Control (*mean difference 1.33 (p = 0.025)*. The Proportionality method yielded a higher number of open-ended design issues than the other methods, that is, points in which the designer stated the need to gain further information through user studies, reference to legislation, or where he or she stated other uncertainties in the design. This observation is confirmed by the interviews of the pilot study, when participants claimed that the proportionality process led them to a point in the design process where they needed further, external validation (in the form of interviews with stakeholders and user studies) for making final design decisions. Insofar adoption of UCD is needed in the design for privacy and security in ubicomp, this can be seen as a positive quality of the proportionality design method.

Number of value propositions (V), between conditions Risk Analysis and Design Rationale (*mean difference = 1.25, p = 0.05*). The higher number of value propositions (V) stated by participants in the Risk Analysis condition is due to a structural effect of one explicit question regarding value proposition in that process. The proportionality method also asks for a value proposition to counterbalance the impact on privacy of the stakeholders, and although the mean of V in the Proportionality condition is similar to that in the Risk Analysis condition, it fails to reach statistical significance at the $p < 0.05$ level.

Quality metric (Q) between conditions Feedback / Control and Risk Analysis (*mean difference = 1.03, p < 0.05*). An interesting observation relates to the Quality (Q) and Grade (G) mean scores of the Risk Analysis condition. The mean scores in this condition are quite lower than those in other conditions, and, in fact, the Q mean difference between the Feedback / Control and Risk Analysis conditions is even statistically significant. This result is even more striking considering that participants in the Risk Analysis condition identified more security and privacy issues than those in the other conditions.

One possible explanation for this discrepancy is that Risk Analysis was the only method that provided a detailed checklist of items to consider during the analysis phase. While guaranteeing that relevant questions are not ignored, this check-list approach may have resulted in dry ‘laundry-lists’ and may have not provided enough space for developing creative designs. Furthermore, few participants in this condition went through the risk management phase due to time constraints, which may have limited their abilities to draft interesting designs. The lack of developed designs may have negatively affected the evaluated quality of the deliverables.

Concluding, the quantitative analysis does not provide strong evidence of differences between the analytic power of the various design methods. In particular, I had hypothesized that at least one of the specialized design methods would have produced a more thorough analysis in terms of number of identified privacy and security issues than the control condition. Although Design Rationale reported lower C and T values, the differences are not statistically significant. On the other hand, my second goal was not of demonstrating the predominance of one method over the others in quantitative terms, but just understanding the effects of the structure of each design method on the resulting analyses. Quantitative analysis provides some insight into these effects. The time spent on the assignment and the prior experience of the participant correlates better with the number of identified issues than the design method used.

The design complexity, C, does not correlate significantly with experience, time nor the design method. This lack of correlation may be in part explained with the volatility of this metric: both complex design requirements and simple requirements (such as password protection) counted as a design choice. However, the correlation of C with the grade indicates that independent evaluators saw differences between designs with low and high C values, suggesting that there is a ‘significant component’ to C apart from analysis noise. My interpretation is that the limited scope, complexity and time allocated to this exercise did not allow participants to complete the designs to a point at which the time they put into the assignment, their experience and the analytic tools at their disposal might have made a difference. While the variable C did not exhaust the expressive potential of the four design methods, variable T did so, if only in part.

5.2.5 Qualitative Analysis

The objective of the qualitative analysis is to identify differences in the type of security / privacy issues brought up by the participants in their designs, as a function of the design method employed. This analysis has been conducted by me, by reading all assignments and coding the privacy and security issues I found according to a classification method described below. The issues were then grouped and further categorized for compiling summary analyses.

5.2.5.1 Identified Issues

I started by reading an assignment, and tagging assertions that could be interpreted clearly as the expression of a privacy or security issue. Then, each issue was compared to a list of issues found in the previous assignments (the list was initially empty). If the issue in question was similar enough to one of those already identified, it was labeled as such. Otherwise, the issue was inserted in the list as a novel entry, rephrasing it in general terms. In cases in which the issue was similar to a previously found issue but did not match exactly, the listed issue's definition was expanded to include both the previously found issue and the one at hand. This process resulted in a list of 61 issues, reported in Table 5.10. Note that these issues were produced by the participants with specific reference to the SenseCam technology and application described above. Each issue was numbered and defined as indicated in the first two columns of the table. The third column indicates the *type* of issue, as defined below in Section 5.2.5.4. The reader will notice that these 'issues' include both potential security and privacy threats in the traditional sense, as well as risks to the well-being and physical security of the people affected by the technology. Moreover, some issues are broad, whereas others are very specialized. Both these effects are caused by the structure of the analysis process.

Two classic problems with this kind of analysis relate to matching and coverage. First, the judgment of whether an issue corresponds to one previously identified is necessarily arbitrary because I did not use formal models for the privacy and security issues. Using such models would have provided more precise results in some cases, but at an exceedingly high cost to the analyst and without the guarantee of being able to model such a wide variety of possible issues, threats and risks. Second, *a posteriori*, some issues may overlap. Controlling this overlap requires the evaluator to define accurately every issue and to proceed with careful classification. An analysis by external, independent reviewers would help increase the reliability of this classification but was not performed at this point due to resource constraints. Notwithstanding these two limitations, the classification reported above allowed me to make interesting observations, including counting the number of unique issues, the most frequent issues, and the type of issues identified in each condition.

Table 5.10: Identified Issues.

Issue	Issue Description	Type
0	Specific to Design – Miscellaneous	Security
1	Wearer does not understand device	Notification
2	Wearer does not understand rights	Notification
3	Impossibility to turn off/control device	Control
4	User is not aware of device operation	Notification
5	Wearer does not understand risks / when to deactivate device	Notification
6	Pictures taken in inappropriate environment	Privacy
7	FERPA-covered data may be collected	Privacy
8	Owner may circumvent notification mechanisms	Notification
9	Capturing same data multiple times	Data
10	Data tamper/destruction by observer	Security
11	Data management burden excessive	Management
12	Others avoid wearer/stigma	Social
13	Capturing irrelevant data	Data
14	Capturing excess data / excessive storage requirements	Data
15	Camera obscured	Control
16	Capturing too little data	Data
17	Wearer does not want to capture / loss of privacy of wearer	Privacy
18	Change of behavior in front of camera	Social
19	Recording of others' health-related information	Privacy
20	Bystander is not aware of presence of camera	Notification
21	Bystander does not understand how camera operates	Notification
22	Recording of pictures of written text	Security
23	Use of photos out of context	Social
24	Maintaining photos permanently	Security
25	Expose data in case of theft/loss / Theft - loss	Security
26	Bystander's information accessed / Taking pictures without permission	Privacy

Table 5.10: Identified Issues. (Continued.)

Issue	Issue Description	Type
27	Intentional surveillance of schools or other people / Misuse of captured info	Privacy
28	Misuse for kidnapping/mugging/harm	Physical
29	Use of data for marketing purposes	Privacy
30	Bribing children to use device	Social
31	Bystander does not understand purpose of use / Lack of trust	Notification
32	Bystander does not know who has access to collected data	Notification
33	Others do not have control on use	Control
34	Curtails plausible deniability	Social
35	Data mining	Privacy
36	Lack of value proposition	Social
37	Removal of device by wearer or others / Assault	Physical
38	Device is distracting to user	Social
39	Data capture about people who do not want it	Privacy
40	Bystanders feel uncomfortable	Social
41	Legal risks	Social
42	Enable mass surveillance	Privacy
43	Hacking / tampering with device or system	Security
44	Replication of personal data	Privacy
45	Increase disputes between parents and school	Social
46	Unauthorized access after capture	Security
47	Unauthorized tampering with information	Security
48	Others forcing user to take pictures / Others taking pictures with the camera	Social
49	Infrared sensor may reveal hidden details	Privacy
50	Risk of physical damage to child (e.g. choking)	Physical
51	Repurposing of device	Social
52	Record interaction that does not affect wearer	Data
53	Damage to device	Physical

Table 5.10: Identified Issues. (Continued.)

Issue	Issue Description	Type
54	Lack of maintenance / supervision / administration	Management
55	Others may become verbally abusive with child about camera	Physical
56	Location tracking of wearer and third parties	Privacy
57	Parents exploiting other children's developmental problems	Social
58	Unintentional disclosure of collected data	Privacy
59	Child unable to request consent	Control
60	Child does not heed to no-capture desires of others	Control

5.2.5.2 Identified Issues by Condition

A first question is whether the issues identified by participants varied based on the condition. Figure 5.8 lists all issues on the vertical axis and shows, on the histogram on the left, the numbers of participants in the respective condition who identified that issue. Different colors relate to the four different conditions.

Participants in some conditions were able to identify a higher number of unique issues than participants in other conditions (see Figure 5.8). The number of unique issues identified by a group of analysts is interesting because it relates to analytic coverage. Clearly, higher coverage is better, but it is difficult to understand how to achieve such coverage. Section 5.2.5.3 reports on this analysis.

The figure also suggests that participants in some condition were more likely to identify certain issues than participants in other conditions. The question ensues whether a certain method leads to identifying certain kinds of issues instead of others. Instead of performing such analysis on the raw data, I performed a summary analysis, by grouping the 61 issues in a smaller number of categories. This analysis is reported in Section 5.2.5.4.

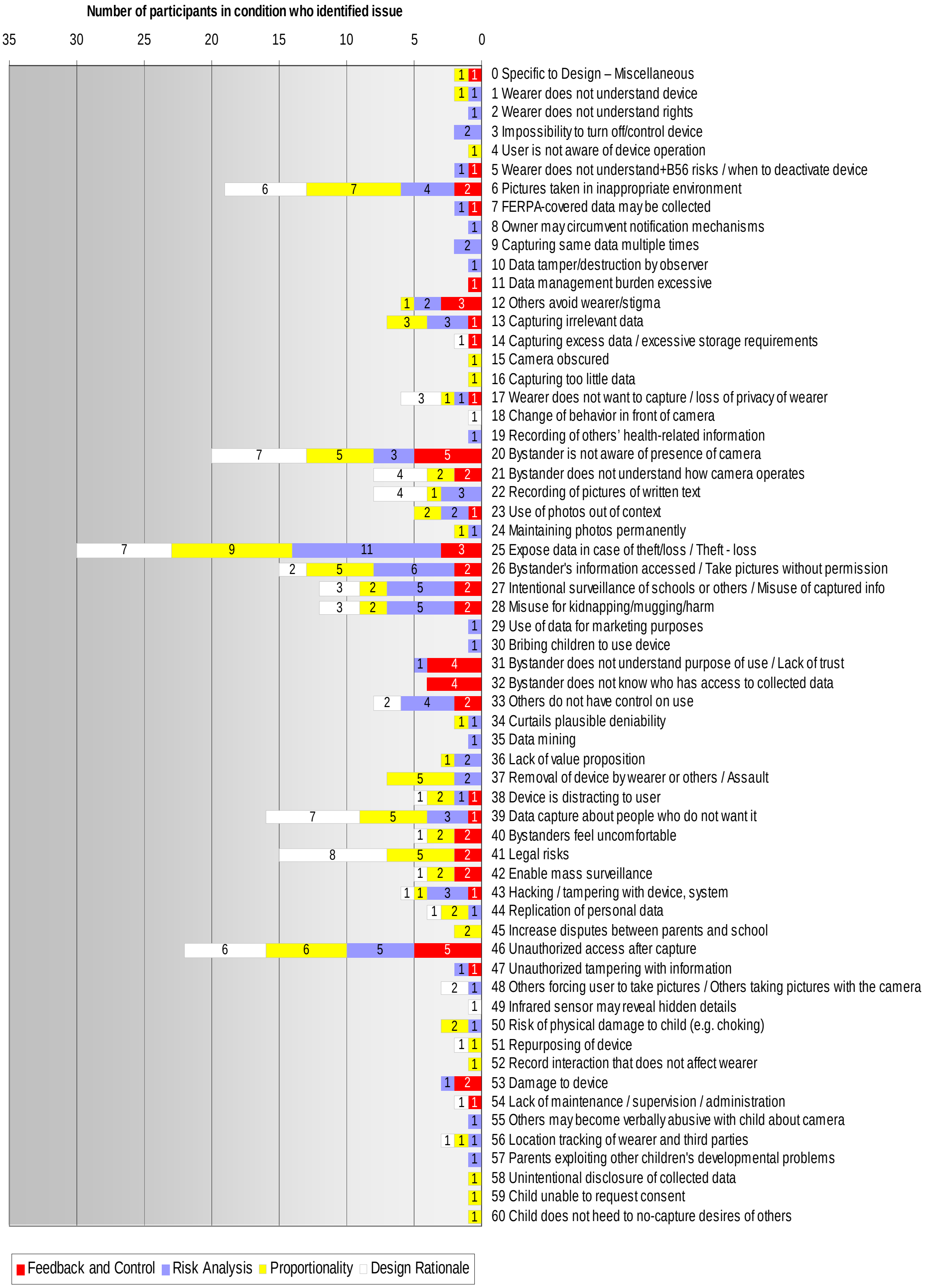


Figure 5.8: Identified Issues and Frequency.

The most often cited issues (*e.g.*, 20, 46, 25, 6) are particularly interesting because they help to understand whether the various design methods reliably help identifying at least this subset of most popular issues. Furthermore, the question arises whether experts would agree that these issues are the most relevant in the context of the SenseCam application. This analysis is presented in Section 5.2.5.5.

Finally, some issues were identified by many participants (in some cases up to roughly half of the participants in each condition), but the majority of issues were found by only one or two participants. Different methods may lead to different analytic *spread*, *i.e.*, situations in which independent analysts identify heterogeneous subsets of issues or where, instead, analysts consistently focus on few, relevant issues. The question of spread is examined in Section 5.2.5.6.

5.2.5.3 Unique Issues

As mentioned in the previous section, the number of unique issues identified by participants in one condition is an interesting metric because it can be used to demonstrate the analytic coverage of heuristic methods (to which all three privacy methods considered here belong), in the spirit of Nielsen's analysis of heuristic evaluation [135]. Table 5.11 shows the number of unique issues identified by participants in each condition. These values are not normalized on the number of participants. A lightweight significance test indicates that the Risk Analysis and Proportionality conditions are signifi-

Table 5.11: Unique Issues.

Condition	**Cumulative Unique Issues**	**N**
Feedback / Control	29	11
Risk Analysis	41	12
Proportionality	37	13
Design Rationale	24	12

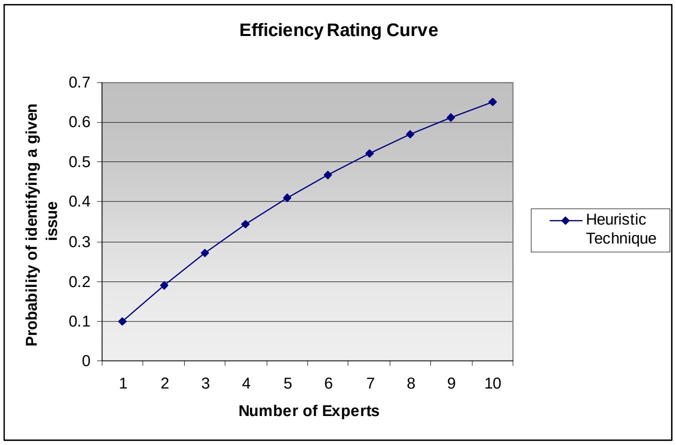


Figure 5.9: Sample Efficiency Rating Curve.

cantly different from the Feedback / Control and Design Rationale conditions.[53] The numbers suggest that the Risk Analysis and Proportionality conditions produced higher numbers of unique issues, corroborating the comments in Section 5.2.4.10 above.

In the case of Risk Analysis the process suggested by Hong *et al.* provides a long list of questions that may have invited participants to come up with a higher number of issues. The effect is less clear in the Proportionality condition, which leaves the task of identifying issues more open-ended. Feedback / Control only concentrates on a subset of privacy issues related to multimedia awareness systems, which may account for the lower number of unique issues identified by participants. Finally, Design Rationale does not suggest particular privacy and security risks for which the analyst should search and this fact can explain the lower number of unique issues identified.

These observations hint at a problem of analysis completeness, a problem common to many domains. Nielsen argued that multiple analysts performing discount usabil-

[53] This significance test was done by taking, in each condition, the unique issues identified by 10 most prolific analysts, those identified by the 10 least prolific analysts, and the average number of unique issues identified by all subsets of 10 designers in each condition. An ANOVA test was then computed on these four sets of 3 samples each.

ity procedures can uncover a large percentage of usability issues [135]. This practice is not unique to the usability community: multiple, independent experts are also used in SE techniques such as Delphi and in IT security engineering. Nielsen used efficiency rating curves to support this claim. These curves assume an independent probability p of identifying a certain usability issue by each expert, and plot the aggregate probability $(1-(1-p)^n)$ of identifying a given issue as a function of the number of experts n (Figure 5.9 shows a sample curve for $p = 10\%$.) These curves suggest that, with enough experts, any issue can be identified with high probability and that the marginal benefit of adding experts to the task decreases with the number of experts. Jensen has used a similar argument in his analysis of the STRAP method *vis-à-vis* Bellotti and Sellen's method [107].

In this case, however, such reasoning cannot be applied in a straightforward manner, because the statistical data obtained in this study suggests that each design method helps the analyst identify only a subset of all the possible issues. For example, the marginal gains obtained by adding participants to the task of identifying privacy and security issues (assuming that the participants who identified the most issues are counted first) decrease to 0 at around 5–7 participants in all four conditions, although at different numbers of unique issues. Note, however, that none of the curves reaches 70% of the total number of all identified issues (see Figure 5.10).

If the inverse graphing strategy is used, *i.e.*, counting first those participants who identified fewest issues, a more linear trend appears (Figure 5.11). Finally, I graphed the *average* number of identified issues, computed on all subsets of 1, 2, 3…13 participants in each of the four conditions (for example, the values for Participants = 3 represent the average of identified issues by all subsets of 3 participants in the respective condition) (Figure 5.12). This graph is similar to the Most-First curves and shows that three out of four trend lines (Proportionality, Feedback / Control, Design Rationale) saturate around participant 10.

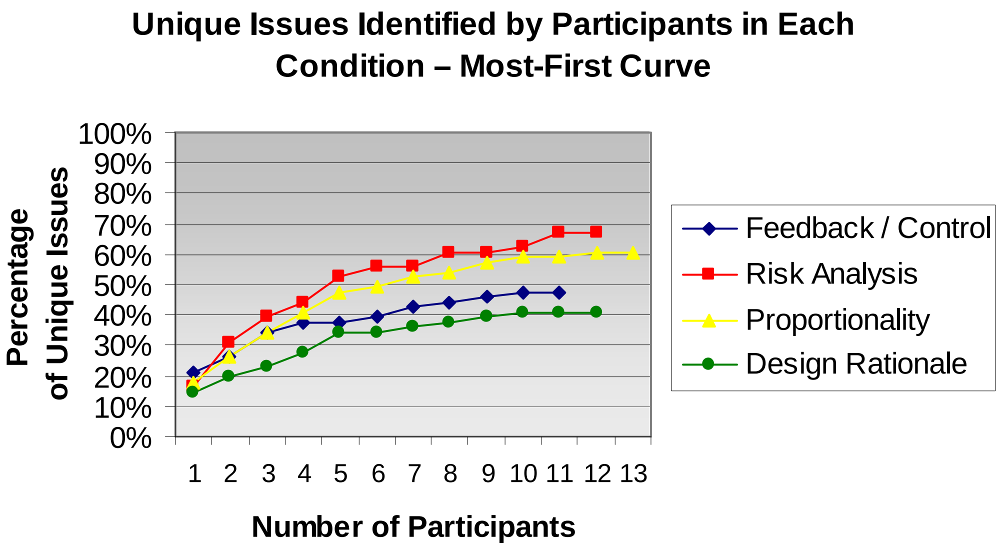


Figure 5.10: Unique Issues Identified by Participants – Most-First Curve.

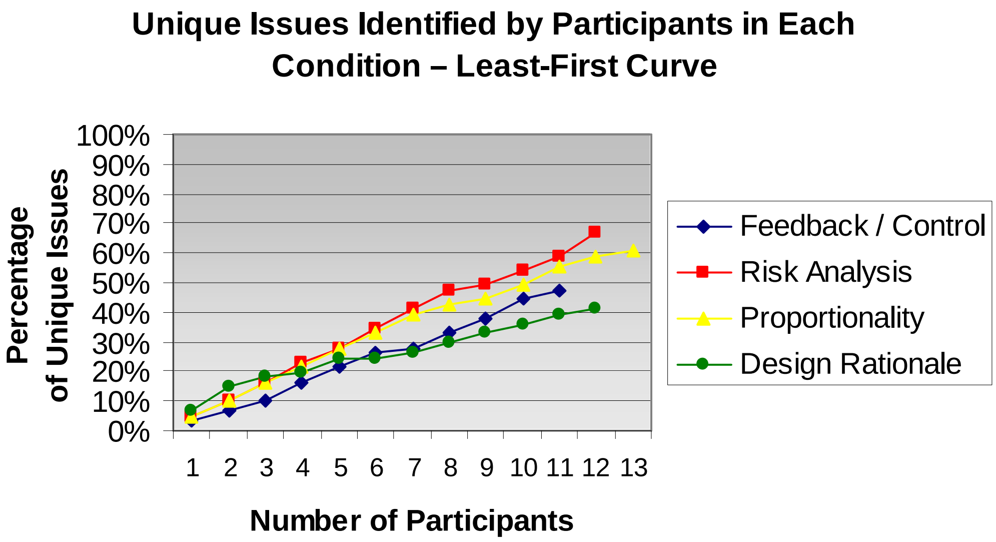


Figure 5.11: Unique Issues Identified by Participants – Least-First Curve.

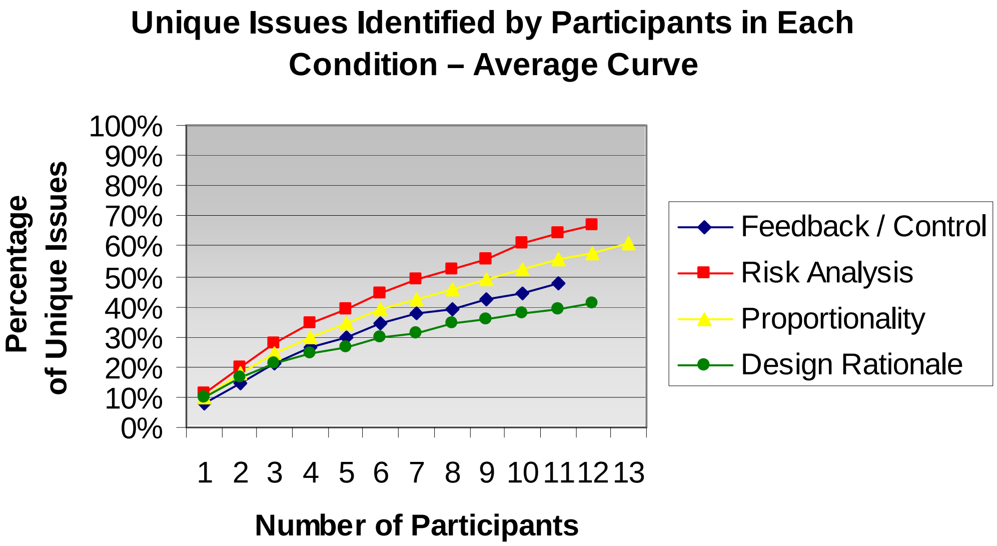


Figure 5.12: Unique Issues Identified by Participants – Average Curve.

One interpretation is that although some methods may help identify a higher number of unique issues, there is no guarantee that a single method can achieve full coverage of the issue space the way Nielsen's efficiency curves suggest, nor that any method is squarely 'better' than the others. This result is due, in my analysis, to a combination of analytic 'noise' (single participants coming up with issues that nobody else sees, *e.g.*, issue 49), and the effect of the four design methods encouraging designers only to look into a subset of potential issues. The analysis of issue type in the next Section suggests that the latter effect may in fact be the case.

5.2.5.4 Types of Issues Identified

The discussion above leaves open the question of what are the different types of issues that each design method helps to identify. Instead of analyzing each issue as a separate entity, I grouped them in eight categories:

– Privacy (general privacy concerns / issues).

– Security (issues pertaining to traditional security: data and service availability, confidentiality and integrity).

Table 5.12: Cumulative Number of Issues Identified by Type in each Condition.

	Privacy	**Security**	**Social**	**Notification**	**Physical**	**Control**	**Data**	**Mgmt**	**Total**
Feedback / Control	11	11	9	16	4	2	2	2	57
Risk Analysis	25	25	11	8	10	6	5	0	90
Proportionality	26	19	17	9	9	3	5	0	88
Design Rationale	25	18	14	11	3	2	1	1	75
Total	87	73	51	44	26	13	13	3	

– Social (potential social problems caused by the device).

– Notification (issues pertaining to notification of collection of data).

– Physical (risks to the physical integrity of the user or the device).

– Control (issues pertaining to control on the collection and use of data).

– Data (data-based issues, *e.g.*, collecting too much data).

– Management (security management issues).

These categories were derived from the source data but their comprehensiveness is confirmed by the fact that they partially overlap with classifications adopted by IT security best practices (*e.g.*, security management standards like IS17799 [104]). The third column in Table 5.10 indicates the classification of each issue. Table 5.12 shows the number of issues of each type identified by the participants in each condition, and overall. Shaded cells indicate numbers of interest that are discussed below. Note that the numbers cannot be compared directly across conditions because of the different numbers of participants in the four conditions.

The most commonly cited issues were those relating to security, privacy, social impact and notification problems. In general, security management issues were not frequent in the participants' analysis. This reflects the general difficulty of forecasting management problems during application design. The type of issues identified relate loosely to the type of questions or heuristics that each design method proposes.[54] The Feedback / Control condition led participants to cite many more notification issues, probably in response to the explicit focus on feedback (notification) mechanisms (this is supported by direct inspection of the design deliverables: most of these issues were listed as response to the questions by Bellotti and Sellen). On the other hand, the participants in the Feedback / Control condition identified a low number of general privacy issues (which include consent, data misuse, *etc.*) and security issues. This may reflect the type of questions addressed by the QOC framework of that method. SenseCam's lack of a user interface may explain the low number of Control issues found by participants in this condition.

Similarly, the Proportionality method suggested to analyze the broader social implications of the technology, especially in the desirability and appropriateness phases, and this may explain the higher number of identified social issues in this condition. In the case of Risk Analysis, many of the issues categorized as "security issues," are directly related to the set of risk analysis and management questions proposed by that method.

The Proportionality and Risk Analysis conditions produced a higher number of physical security issues than the other conditions, probably due to the suggestion in the methods to consider the broader effects and potential side-effects of the technology.

An interesting observation relates to issues of data quality (type "Data"), *i.e.*, collecting irrelevant data, excess data, unusable data or too little data. Participants in the Risk Analysis and Proportionality conditions mentioned more data quality issues than participants in the other two conditions. Data quality is an interesting category because it

[54] Chapter 3 lists the questions and criteria suggested by the Feedback / Control and Risk Analysis methods. Chapter 4 lists the questions of the proportionality method.

is part of the FIPS and affects the usefulness judgment of the technology, but is otherwise rarely seen as a security issue in the traditional sense. The focus on “value proposition” and “balancing” in Risk Analysis and Proportionality may have prompted participants to consider this issue (Risk Analysis even asks: “How much information is shared?”).

5.2.5.5 Most Frequently Identified Issues

The most frequently identified issues are worthy of their own analysis because they introduce the issue of analytic consistency of the design methods. Looking at the issues that were identified by the greatest number of participants in each condition may help develop claims regarding the kind of analysis that each method consistently favors. Focusing on the most frequent issues eliminates those “stray” issues that were identified by one or two participants, and which might have been identified due to analysis noise or other factors such as personal experience. Table 5.13 lists all privacy and security issues identified by at least ⅓ of the participants in one or more conditions (this proportion was selected to provide a reasonable number of “most frequent issues”). The percentages in the cells indicate the portion of participants in each condition who identified the respective issue. Cells with percentage 33% or higher are shaded.

It is worthwhile to note that only one issue has been identified by at least one third of all participants in all conditions—“Unauthorized access after capture.” Considering the scope and type of issue, it appears to be a reasonable candidate as the most prominent issue. Three further issues, 6 “Pictures Taken in Inappropriate Environment,” 20 “Bystander Not Aware of Camera” and 25 “Expose Data in Case of Theft/Loss” were identified by ⅓ of participants in three of the four conditions.

A first observation relates to the relevance and type of the most frequently identified issues. The Risk Analysis, Proportionality and Design Rationale conditions present a higher degree of coverage of the most prominent issues. It is interesting to note that in this respect, the Feedback / Control condition produced lower coverage of prominent issues. This is in part attributable to the analytic framework proposed by that method—issues such as Theft (25), Disagreement (39), Third Parties (26), *etc.* are not explicitly contemplated by that framework. In this respect, it appears that Bellotti and Sellen's Feedback / Control framework, borne from a specific type of ubicomp application, may not perform as well as more general approaches in identifying relevant privacy / security issues in a different type of application (one obvious difference between the RAVE system and SenseCam is the mobility of the latter).

Design Rationale left participants unaided in discovering issues and this may have helped them identifying consistently the more popular issues overall because they were free to think about the application without having to respond to specific design questions. However, some issues identified often by participants in that condition are arguably of secondary importance in this application context (*e.g.*, "Record pictures of written text").

Another way of looking at this data is that of cataloging the intentionality of the threat associated with a specific issue. Issues marked with an asterisk (*) in Table 5.13 indicate that the issue requires an intentional action by a threat agent to become a real threat. Risk Analysis is correlated with the consistent identification of more issues of this kind than Proportionality and Design Rationale. Again, this may be explained by the specific questions asked in the Risk Analysis analytic framework.

An interesting consideration relates to the issues that are *not* in Table 5.13: were important issues consistently overlooked by these participants? I did not perform an expert analysis of this application to compile a set of important privacy and security issues usable as benchmark. However, as a first approximation, I employed the list of all identified issues (Table 5.10) as benchmark. A summary examination of that list suggests that few relevant issues in the context of this application were left out by more than ⅔ of the participants in all conditions. This suggests that the issues in Table 5.13 are not only the most popular, but also include many of the most relevant. An independent evaluation by experts would improve the trustworthiness of this conclusion.

Table 5.13: Issues Identified by 33% or More Participants in at Least One Condition.

Issue	**Type**	**Feedback/Control**	**Risk Analysis**	**Proportionality**	**Design Rationale**
46 Unauthorized Access After Capture *	Security	(45%)	(42%)	(46%)	(50%)
6 Pictures Taken In Inappropriate Environment	Privacy	(18%)	(33%)	(54%)	(50%)
20 Bystander Not Aware Of Camera	Notification	(45%)	(25%)	(38%)	(58%)
25 Expose Data In Case Of Theft/Loss	Security	(27%)	(92%)	(69%)	(58%)
26 Access To Bystander/Third Party Data	Privacy	(18%)	(50%)	(38%)	(17%)
39 Capture Of Data Of People Who Do Not Agree	Privacy	(9%)	(25%)	(38%)	(58%)
41 Legal Risks	Social	(18%)	(0%)	(38%)	(67%)
21 Bystander Doesn’t Understand Device Operation	Notification	(18%)	(0%)	(15%)	(33%)
22 Record Pictures Of Written Text	Security	(0%)	(25%)	(8%)	(33%)
27 Intentionally Monitoring School *	Privacy	(18%)	(42%)	(15%)	(25%)
28 Misuse For Kidnapping / Mugging *	Physical	(18%)	(42%)	(15%)	(25%)
31 Bystander Doesn’t Understand Purpose Of Use	Notification	(36%)	(8%)	(0%)	(0%)
32 Bystander Doesn’t Know Who Has Access To Data	Notification	(36%)	(0%)	(0%)	(0%)
33 Third Parties Do Not Have Control On Use	Control	(18%)	(33%)	(0%)	(17%)
37 Removal Of Device By Others / Assault *	Physical	(0%)	(17%)	(38%)	(0%)

** Cells with 33% or higher are shaded.

5.2.5.6 Issue Spread

The distinction between prominent issues from those identified occasionally leads to the question of how focused each design method is. Table 5.14 reports “analytic spread,” *i.e.*, the ratio between unique (Table 5.11) and the total number of issues identified by participants (last column of Table 5.12) in each condition. This value indicates how *focused* the analysis performed by participants was on a subset of issues (lower values indicate higher focus). Higher spread indicates a higher variance of issues raised between participants in a given condition. In general, these values are in accord with the data in Table 5.13: participants in the Feedback / Control condition identified less prominent issues, with higher spread and participants in the Design Rationale condition presented lower spread and more focus on few prominent issues. (Note that the “Total Cumulative Issues” and “Spread” numbers in Table 5.14 have not been tested for statistical significance).

Participants in the Feedback / Control condition identified less unique issues than participants in other conditions. Participants using Design Rationale identified roughly as many total issues as participants in the Risk Analysis and Proportionality conditions but focused on a smaller number of unique issues; this is interesting because it suggests that without specific guidance, participants identified almost the same amount of issues as

Table 5.14: Issue Spread.

	Unique Issues in Condition	**Total Cumulative Issues**	**Spread (unique issues / total cumulative issues)**
Feedback / Control	29	57	0.51
Risk Analysis	41	90	0.46
Proportionality	37	88	0.42
Design Rationale	24	75	0.32

other groups but were less “creative” in doing so. Participants in the Proportionality and Risk Analysis conditions identified similar numbers of total issues, with the Proportionality conditions showing a slightly higher spread.

A high spread can be viewed both positively and negatively. High spread may indicate that the design method prompts designers to explore more diversified issues, increasing “analytic reach.” Since these participants did not have enough time to exhaust the analysis of the application, they might not have reached a level where they started identifying the same issues. Given more time, methods with high spread may result in the identification of more issues. A high spread is however a risk to consistency, because it weakens the claim to predictability of the outputs of the analysis activity.

Conversely, low spread may be positive for consistency: every designer using the same method tends to find the same issues. However, low spread also suggests that even by adding more experts to the task of identifying issues and giving them more time, they may still not find all possible issues.

5.2.6 Subjective Metrics

In this section, I present summary results on the participants’ subjective assessment of the perceived usefulness and usability of the four methods to complete the homework assignment, on the time it took them to complete it and on the stability of their opinions and preferences about privacy.

5.2.6.1 Perceived Usefulness and Usability of the Four Methods

Table 5.15 shows the self-reported statistics on the perceived usefulness and usability of the design methods as probed in the post-questionnaire. Although none of the differences in the averages is significant according to an ANOVA test, due to the high variance, it is interesting to observe that Design Rationale scored lowest on the usefulness question, and highest on the ease-of-use question.

Table 5.15: Perceived Usefulness and Usability of Design Methods.

Question	**Control / Feedback**	**Risk Analysis**	**Proportionality**	**Design Rationale**	**Total**
The design method was useful to me in this assignment. (0: strongly disagree, 6: strongly agree)	mean = 4.3 σ = 1.5	mean = 4.5 σ = 1.6	mean = 4.4 σ = 1.3	mean = 3.9 σ = 2.2	mean = 4.3 σ = 1.7
The design method was easy to apply. (0: strongly disagree, 6: strongly agree)	mean = 2.9 σ = 2.0	mean = 4.0 σ = 1.8	mean = 3.6 σ = 1.6	mean = 4.2 σ = 1.8	mean = 3.7 σ = 1.7
I would use the design method again in the future for similar design tasks. (0: strongly disagree, 6: strongly agree)	mean = 3.5 σ = 1.4	mean = 4.3 σ = 1.4	mean = 4.4 σ = 1.8	mean = 4.2 σ = 1.9	mean = 4.1 σ = 1.6
How did the design method affect the quality of your assignment? (0: greatly increased, 6: greatly decreased)	mean = 2.6 σ = 1.7	mean = 3.5 σ = 1.2	mean = 3.3 σ = 1.9	mean = 1.8 σ = 1.6	mean = 2.8 σ = 1.7
How did the design method affect the time it took to perform the homework? (0: greatly increased, 6: greatly decreased)	mean = 1.8 σ = 1.9	mean = 1.6 σ = 1.5	mean = 2.7 σ = 1.7	mean = 2.6 σ = 1.3	mean = 2.2 σ = 1.6

Risk Analysis and Proportionality scored lowest on the perceived improvement of the quality of the assignment (note that the scale is inverted for consistency reasons with other questions on the survey). In any case, they scored barely worse than the mid point (which was labeled “did not increase nor decrease”). It is interesting to note that the self-assessed measure of quality across conditions is somewhat parallel to the evaluators’ quality metric Q in Table 5.9 (in fact, there is a weak, non-significant correlation).

Participants in all four conditions indicated that using the respective design method increased the time needed for the assignment (especially in the Feedback / Control and Risk Analysis conditions). This is interesting because it contrasts with interview responses and written comments on the questionnaires, where participants noted that having a standard procedure to follow relieved them from having to plan the steps needed for performing the homework. On the other hand, many participants complained that the homework was too complex and lengthy for the available time. Recalling the comments made in the pilot study interviews, the correct interpretation of this contradiction may be that, while having a standard procedure reduced planning time, satisfying all the steps required by such procedure took more time than what they would have otherwise spent on the assignment.

Note that the self-assessed data on time reflects in part the homework execution time TT in Table 5.8 (again, there is a weak, non-significant correlation). For example, the perception of the increase in time required to complete the assignment by participants in the Proportionality condition was the lowest. These participants took the least time in completing the assignment.

5.2.6.2 Participants’ Change of Privacy Preferences

On average, participants stated that their opinions on privacy and security had not changed because of participating in this study (“Working on this assignment changed my opinion about technology and its social implications.” 0: strongly disagree, 6: strongly agree; mean 3.0, $\sigma = 1.7$, no significant difference across conditions). This is part supported by the stability of the Harris-Westin survey taken before and after the assignment was made. Only 13 participants changed their Westin classification, and in all cases these were borderline switches.

It should be noted, however, that the Harris-Westin classification scheme may not be particularly suited to characterize the privacy opinions of participants with reference to this study, because it relates to individuals *vs.* organizations as opposed to personal applications such as the target of the homework in this study. Moreover, the Harris-Westin is intended for probing the opinions of *consumers* and not designers.

5.3 Discussion

What conclusions can be drawn from the results this evaluation, specifically in reference to the thesis outlined in Chapter 1? Although many of the results presented above are not statistically significant, it is still possible to infer a number of interesting conclusions.

Participants in all four conditions took approximately the same amount of time to complete the assignments and many indicated that the assignment scope was broader than what they could accomplish in the allotted timeframe. This, and the high spread measures reported in Table 5.14 above suggest that the participants did not individually exhaust the “analytic potential” of any of the four design methods (*i.e.*, they did not reach the point where no further security and privacy issues could have been identified, and design choices made). They also did not exhaust the *design space*, (*i.e.*, the number of aspects of the design and application that were available for consideration) as indicated by the low ratio between identified issues by any participant and total identified issues.

Thus, the results are bound by the available time. One may question whether it is fair to evaluate design methods, that by definition are meant to be used over long periods, in a time-limited experiment. One approach would have been to allow designers more time—a month or two (as was done in the pilot study). At the other extreme, are time-constrained evaluations of performance. For example, Chung *et al.*'s evaluation of patterns was limited to 80 minutes, both for expert and novice designers; in Jensen's evaluation of STRAP, participants took 80–100 minutes to complete the analysis. It is true that design tasks in the real world enjoy limited budgeting and staffing and that IT developers commonly lament lack of both. However, design and analysis, even of very simple applications such as SenseCam, are complex activities that require time to perform accurately. Limiting evaluation to one or two hours may not result in an accurate picture of how designers work in practice. In this respect, I believe that the setup of this study strikes a middle ground between a drastically time-limited "race to find the issue" and an unbounded analysis.

Time spent on the assignment, as well as the experience of the participants, appear to be important determinants in the comprehensiveness of the analysis. There is significant correlation between the time needed to complete the assignment and the number of security and privacy issues identified. The experience metric is also correlated with the number of identified issues. This suggests that participants with extensive prior experience were somewhat facilitated in the analysis. On average, these two factors appear to be more influential than the specific design method employed, suggesting, again, that the limits of the design methods were not reached.

However, the number of identified privacy and security issues cannot be taken as the best or only way of evaluating the design products, as suggested by the lack of correlation between the evaluators' quality judgment with the number of identified issues. The relevance of issues as well as more general concerns regarding issue coverage and heuristics' efficiency are as important in evaluating a design method.

In this respect, the qualitative analysis provides even more compelling insight than the quantitative assessment: the issues that were identified by the participants were related to the analysis questions proposed by the three privacy-specific design methods.

Lacking this support, participants in the control condition identified less unique privacy and security issues. Analytic coverage (the percentage of identified issues by all participants in one condition relative to all issues) of each method appears to be limited, and it is not clear whether any one method would help identifying all the issues that were mentioned by the participants—ideally, two or more design methods covering different aspects of the design space should be used together, by multiple analysts, to obtain high coverage and a high probability of identifying relevant issues.

Such a compound design method could combine general questions, such as those proposed by the proportionality method, with a risk analysis approach and domain-specific questions such as those proposed by Bellotti and Sellen.

The lack of concern for security management in the participants' designs—both of experienced and inexperienced participants—though expected, is worrying. Security management is today considered one of the most challenging aspects of information systems' security, and ubicomp technology will bring a whole new scale to the problem. The worry is not that the participants did not raise management issues—after all, a majority of study participants were students with scarce professional experience, and security management is (unfortunately) not taught in class. What is worrisome is that none of these "design methods" managed to push the problem of management to the forefront of the designers' attention. In truth, the proportionality method suggests to consider management issues during design, but that observation is buried in the method's description and may not be prominent enough. One conclusion is that management should be promoted to a major item of concern in future design methods in this domain.

5.4 Thesis Coverage

Let's return now to the proportionality method and reconsider the thesis statement of Chapter 1. My personal experience with the case studies of Chapter 4 and the two studies documented in this Chapter provide some material for arguing the various claims.

Thesis Claim 1, that the proportionality method can be employed in the design of ubiquitous computing applications, is in my judgment supported not only by own experience in the case studies, but also by the results of both the pilot and the evaluation studies. The proportionality method was usable by participants of the pilot study. The proportionality method was used by participants in the second study along with other similar design methods, with good results in terms of quality, comprehensiveness, issue coverage.

Thesis Claim 2, that it "supports requirements analysis by indicating pertinent research questions targeted at improving the understanding of applications and their usage context" is supported, again, by my own experience documented in the two case studies and by study participants. Participants in the pilot study spontaneously commented that it helped them frame research questions and communicate in a way that is convincing to external people. Though encompassing less steps than Risk Analysis, the proportionality method fared comparably in the number of identified privacy and security issues (which I use as a proxy for "requirements analysis" in the thesis claim), and brought many more participants to state the need for external reference than the other methods.

Thesis Claim 3, that it helps "select the most appropriate alternative among design options" was not demonstrated. Informal evidence gained in the analysis of the design products in the two studies suggests that it helped decide among design options, but not that the choices made by designers are the most appropriate. At this point, there is not sufficient evidence to support this claim, also because confirming it would require further evaluation of the design decisions taken by participants.

Thesis Claim 4 (generality across individuals) is in part confirmed by the informal analysis of the design deliverables, where participants followed the steps suggested by the method's description. However, the average Adherence score of the Proportionality condition is relatively low at 0.71, due to many participants skipping the adequacy phase probably due to lack of time. Issue spread, which I used to indicate the level of consistency across designers, is the second lowest among the four conditions, at 0.42. Overall, there is not sufficient evidence for confirming or disproving this thesis.

Thesis Claim 5 (acceptable cost) is supported by the data collected in the second study. Participants using the proportionality method employed approximately the same time as participants in other methods, with similar if not better performance in terms of identified issues, grade and quality.

Thesis Claim 6 (better performance) could not be demonstrated conclusively. Data shows that the performance of the proportionality method with relation to variable T is very close to that of Hong *et al.*'s risk analysis, and better than Design Rationale and Bellotti and Sellen's framework. The difference in means is not statistically significant. However, proportionality also scores high both in the cumulative total number of identified issues (see Table 5.10), and in the coverage of the top 15 issues (see Table 5.13).

Concluding, while it seems that the proportionality method may have not fared significantly better than the other methods in quantitative terms, this evaluation suggests a path for further research, which combines one or more methods to achieve superior results—specifically, a general design method such as the proportionality method combined with a heuristic method such as the Bellotti's framework. This argument is further expanded in the last Chapter.

CHAPTER 6

TOOLS AND TECHNIQUES

In the introduction, I argued that a tighter integration of UCD principles in the domain of ubicomp privacy and security is necessary for bridging the acceptance gap facing the development of these technologies.

In Chapter 4, I compared the proportionality method to a scaffolding structure that invites the designer to ask questions about the stakeholders, the application and its design, but does not indicate a response to those questions. The evaluation in Chapter 5 provided hints that this scaffolding structure indeed accomplishes its purpose of motivating a user-centered approach to security and privacy analysis. In particular, the participants using the proportionality method in the second evaluation study referenced the need for external inputs and validation (which includes probing users' opinions, evaluating the technology in deployments, analysis of legislation, *etc.*) statistically more often than participants in other conditions. This suggests that the proportionality method encourages designers to adopt an inquisitive approach to design in this domain, potentially furthering UCD.

Therefore, the question becomes how to integrate, *in practice*, user inquiry and a broader consideration of requirements into privacy and security-enhancing design. Usability and security are a tough mix, and often compete for what remains of a product development budget once as many features as possible have been designed and performance maximized. In *Seeing What's Next*, Christensen *et al.* argue that non-functional aspects of design (such as usability or privacy) are relevant, from a business standpoint, only for a short window in most products' lifecycle, after the product has matured but before competition shifts to price [44].

This Chapter attempts to address these questions: how do we identify the most relevant questions affecting adoption, security and privacy in a timely manner? How do we demonstrate their relevance and how do we go about answering them? And, finally, how do we integrate the acquired knowledge back into application design? Below, I present some techniques that I have used in the past few years in connection with the case studies described in Chapter 4. Instead of discussing how the proportionality method was applied in the two studies, as done above, I discuss here more general issues, including the advantages and disadvantages of the techniques I used. There is no silver bullet, and I do not claim that my experience generalizes to all ubicomp applications—the intent in this Chapter is to start reflecting on the application of user-centered design in the domain of privacy and security in ubicomp, with the hope that these observations may be useful for solving similar problems in the future.

6.1 Using Surveys Probing Privacy and Security Questions

In Chapter 4, I noted that in order to make strong claims within the proportionality method, reference to the user and the application's purpose is necessary in addition to considering technical and legal issues. Surveys are a popular way of probing the opinion of people about a technology and are widely used in the HCI community. Surveys represent a low-cost method for gathering statistically significant information about users' preferences and opinions. However, privacy and security are elusive topics to survey, because often the behavior of people differs from what they say when asked about them.

In Chapter 3, I claimed that many people assume a deontological stance towards privacy for many reasons, including insufficient informational awareness, overriding primary goals or carelessness. On the other hand, people have a very refined sense of privacy in interpersonal relations, as described by Altman [20], and may choose certain paths of behavior to avoid conflict or in response to overriding social goals. In some cases, however, they may be unable or unwilling to explain their behavior, due to many reasons. Behavior in specific circumstances may be difficult to generalize; second, it may be difficult to express openly (*e.g.*, the need for plausible deniability in social relations is well known [54], but people may not want to admit it); and thirdly, we may be unaware of certain dynamics because they are so engrained in our daily behavior.

Security is often perceived as an impediment to effectiveness and many organizations handle data differently from how a straightforward security system assumes. Povey argues that any security system should provide escape mechanisms that allow users to complete transactions, in exceptional circumstances, that would be otherwise forbidden [147]. Povey claims that by employing audit and redress, social forces can prevent misuse even without strict technical control, while still allowing for exceptions. He calls this policy "Optimistic Security." I would argue further that in many instances there is a mismatch between day-to-day behavior and idealized (and often overly strict) security frameworks, and that this is one of the reasons why many security systems fail—a similar rift exists between written policies and actual practice in some ISO9001-certified organizations. Asking people in a survey how their "security system" works (be it in an organization or in private life) may likely result in them describing the way it *should* work, and not how it really works. These observations suggest that surveys must attempt to investigate the "action behind the opinion."

In Chapter 2, I distinguished the "personal privacy" approach to privacy issues from the "data protection" approach. These distinctions are relevant also when using surveys to probe privacy attitudes. Personal privacy focuses on interpersonal relations, that most individuals manage continuously as a natural matter of life, influenced by the social context, the quality of the interpersonal relationship and the purposes of the activities being achieved. As mentioned above, many details of the social relationships involved in personal privacy may go unexpressed in the standardized questions of a survey. To probe these details, researchers should attempt to capture the actual manifestation of privacy preferences and attitudes and focus on specific instances of interpersonal interchanges (for example, in the Personal Audio Loop Diary study interviews, we tried to survey opinions always in relation to a specific incident of use of the application). In fact, tools such as ethnographic inquiry, experience sampling procedures, or evidence-based focus groups may represent more informative investigative tools, as discussed further below.

On the contrary, data protection rests on the accurate definition of data management processes and on the specification of privacy preferences and procedures. Given that data protection issues arise in conjunction to large numbers of individuals, surveys appear as an appropriate tool for probing a social group's preferences (*e.g.*, the GVU WWW User Survey [83], the PB&A Survey [149]). Here, one fundamental evaluation challenge rests in the ability to convey, to non-expert users, sufficient information to express reasonable and informed preferences and attitudes (as attempted by Günther and Spiekermann in their recent survey on RFID privacy preferences [82]). As Adams and Blandford point out [17, p. 180], risk management is hard for individuals who do not have sufficient information to evaluate the graveness and likelihood of a certain threat—*e.g.*, how does the retention time of financial information by credit rating organizations affect identity theft? Even experts may be unable to state informed and realistic policies in such settings. The way these threats are presented to the surveyed participant may strongly influence the outcome of surveys and is a serious roadblock to gathering reliable data for design. Furthermore, surveys can fail to consider *scale*: asking whether an individual desires tight control on certain information disclosures may not be representative of the individual's day-to-day handling of hundreds of information disclosures. In this context, it is interesting to note that one of the main weaknesses of data protection legislation is in long-term control and scalability. Not only are individuals *unaware* of their rights, as noted in a 2003 EU Commission report [49], but they also tend to *forget* of all the parties to which they consented disclosing data.

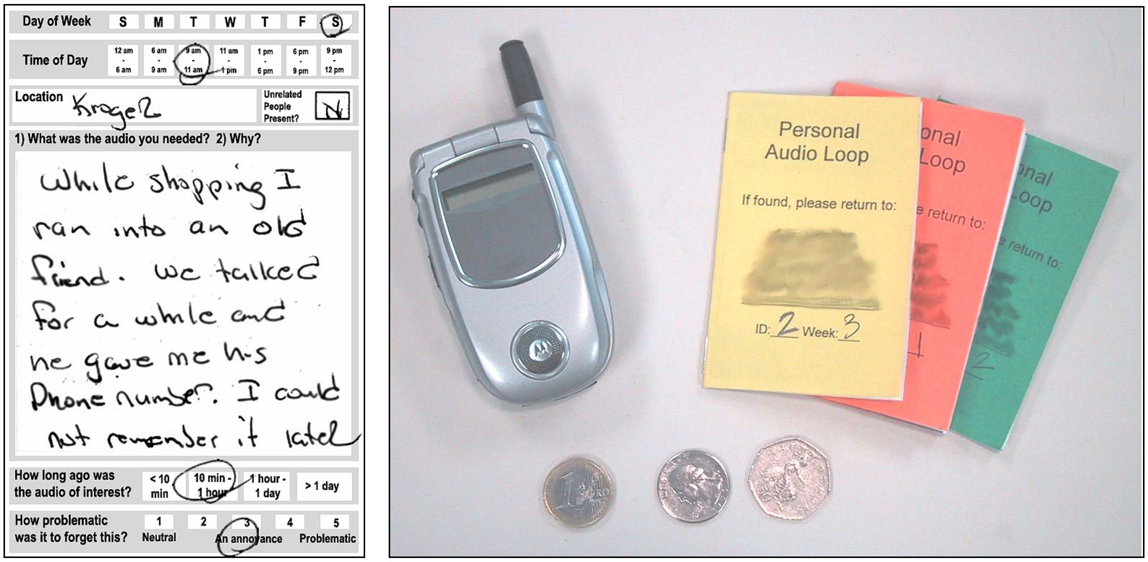
Summarizing, surveys may be a cost-effective way of gathering information about user preferences and opinions, but the researcher should beware that results may differ significantly from how people may act when faced with the same situation in the real world, both when considering personal privacy and information transactions with data protection concerns.

6.2 Beyond Surveys: Using Experience Sampling to Probe Privacy and Security

In light of the problems detailed above, I have come to question the descriptive power of abstract surveys on privacy and security, even accounting for their cost advantages. Studies that probe users more closely, such as ethnographic observation, can produce more accurate results. In addition to providing grounding for determining legitimacy, appropriateness or adequacy of an application, such studies help to understand how users might adopt the application, and its social effects.

Even adopting these inquiry tools, the problem remains that people may be unable to grasp immediately the security effects of new technologies on their existing socio-technical practices: ubicomp technologies are often difficult to imagine in operation, and in addition, security or privacy-enhancing functions may not be employed immediately. However, observing use in a long-term deployment may be a costly endeavor. We thus have a chicken-and-egg problem in that “authentic” observation of people’s behavior and opinions probed in realistic conditions is necessary for informing design, but a certain level of technology is necessary for allowing people to understand what is being asked.

In part as a response to this problem, Experience Sampling Method (ESM) studies are becoming increasingly popular in HCI practice, often in association with diary studies, to probe privacy questions. Experience sampling is a self-reported inquiry technique that has long been used within behaviorism, medicine, and industrial psychology. Larson and Csikszentmihalyi were among the first to propose experience sampling as a quantitative self-reported inquiry technique [117] for social and psychological research. Wheeler and Rois described the use of experience sampling techniques in many domains,



Day of Week	S	M	T	W	T	F	[✓ S]
Time of Day	12 am - 6 am	6 am - 9 am	[✓ 9 am - 11 am]	11 am - 1 pm	1 pm - 6 pm	6 pm - 9 pm	9 pm - 12 pm

Location KrogeR Unrelated People Present? N

1) What was the audio you needed? 2) Why?

While shopping I ran into an old friend. we talked for a while and he gave me his Phone number. I could not remember it later

How long ago was the audio of interest?	< 10 min	[✓ 10 min - 1 hour]	1 hour - 1 day	> 1 day

How problematic was it to forget this?	1 Neutral	2	[✓ 3 An annoyance]	4	5 Problematic

Figure 6.1: The PAL diary.

and categorized them in: interval-, signal- and event-contingent, depending on what initiates the self-report procedure [181].

Prior to the Reno deployment, Consolvo *et al.* conducted a signal-contingent experience sampling to study the privacy issues involved in disclosing one's location on mobile terminals [51]. In their study, participants carried a Palm device that simulated, at random times, location requests from friends, family and colleagues. Consolvo *et al.* point out that these random simulated requests were in various occasions implausible from a social standpoint. Nevertheless, they were able to obtain interesting data on their participants' privacy preferences that would have been difficult to obtain using a normal paper survey.

The PAL Diary and Proxy studies described in Chapter 4 both employ event-contingent experience sampling procedures. In the Diary study, the event prompting the survey was the hypothesized instance of use of the application (*i.e.*, when the user desired to re-listen to audio he or she heard in the near past). Figure 6.1 shows a sample diary entry compiled for each event by the diary study participants, including salient questions about the application usefulness and potential privacy implications ("were other people present at the recording?," "how long ago did the event happen"). The diary was purposefully made to mimic the form factor of the phone on which we had developed the PAL application (picture on the right). Each diary contained several event pages and was replaced every week during the study. The diary entries were utilized in weekly interviews to provide factual foundation to questions about the hypothesized use of the application. Appendix B contains the interview templates we used in the weekly interviews, where we probed both a selection of specific events and general opinions.

In both this study and the Proxy study, we were able to gain credible insight into the privacy preferences of the participants in socially plausible situations. Using event-contingent instead of signal-contingent procedures allowed us to increase the plausibility and realism of the probed situation.

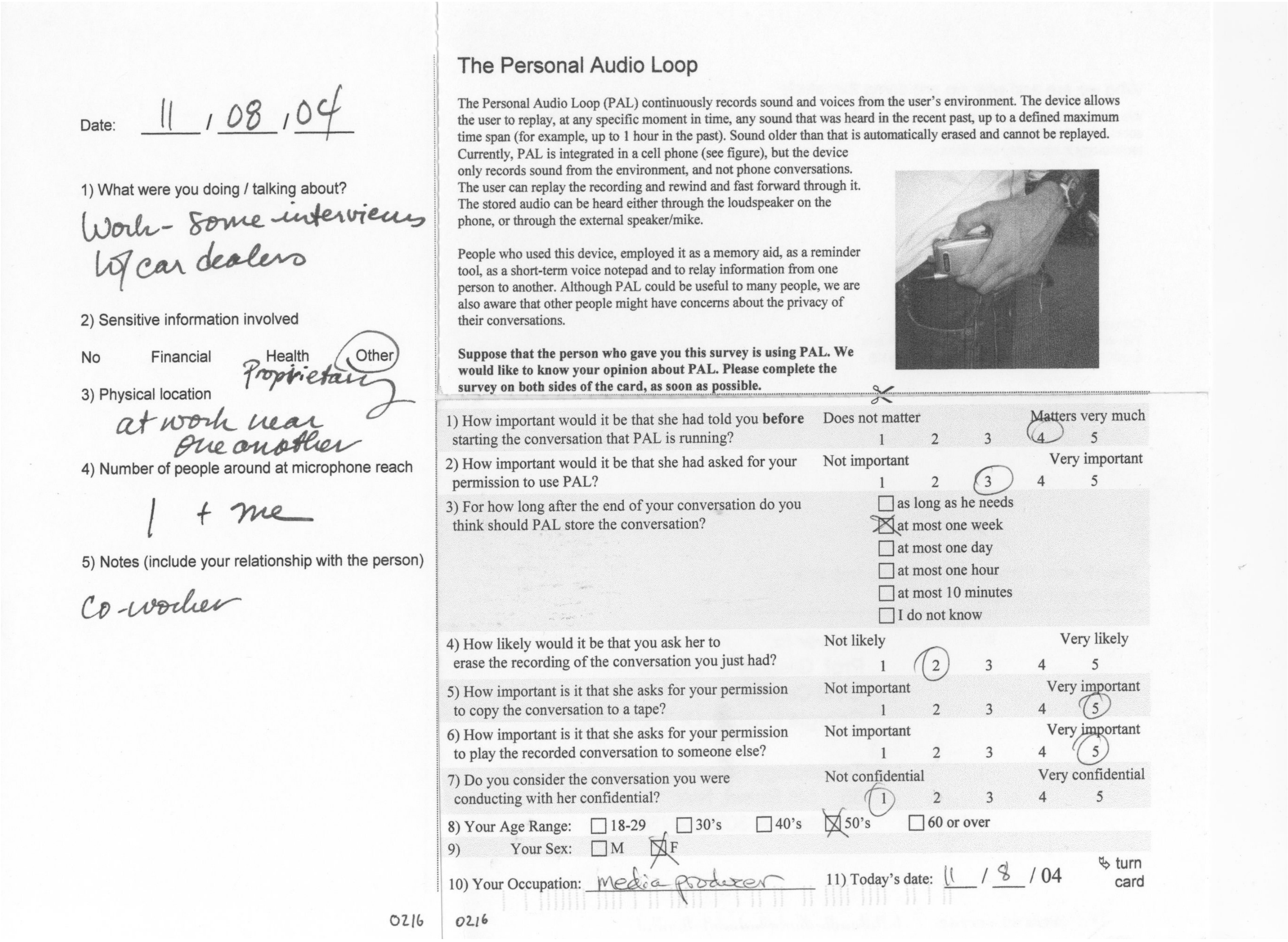
6.2.1 "Paratypes:" Combining Experience Sampling with Experience Prototyping

In the PAL Proxy study, the survey was also prompted by an "event"—the conversation occurring between a hypothetical user of PAL and another person. However, the Proxy study went further than merely sampling participants' experience. When the investigator (the proxy) handed out the survey, he or she asked the participant to imagine that he or she had been using PAL. This allowed us to *prototype an experience*,[55] with a concrete reference to an instance of real life, and to sample the participant's opinion on that instance. I called this procedure a *paratype*: a simulation, or model, of interaction ("-*type*") with a technology which is evaluated alongside ("*para*-") real-world experience.

[55] Buchenau and Suri published an article on Experience Prototyping [41], where they claim that role playing can be useful for understanding the social context in which a person will use a technology. Their approach creates artificial experiences (*e.g.*, by building a reproduction of a plane interior, or by role playing during a train journey). In the PAL Proxy study, we attempted to use the actual experience of the participant, as it would have happened without the study.

This procedure allowed us to situate participant response in the experience the person just had, with a specific partner, conversation topic and location, supposedly reducing recall errors and hypothetical answers. That the survey was administered by human proxies is not part of my definition of paratype. The term paratype only refers to introducing simulated interaction with a certain technological artifact within a specific setting of real social action, and documenting the effects of this combination. The proxy's role was only incidentally that of administering the survey—the main function of the proxy was that of acting as "PAL's user" and as interaction counterpart of the participant. In this sense, the proxy's role was to *create the instance of technological interaction* on which we wanted feedback, with the help of the description of the application and, upon request, a demonstration of the working device. Event-contingent experience sampling was deemed a particularly suitable way of documenting participant feedback in this case.

Figure 6.2 shows the PAL proxy survey. The survey form is divided in three parts, here shown after being reassembled. The right side was given to the participant after the conversation with the proxy had occurred. It contains a description of the application and the survey (the descriptive text is reported in Appendix B for enhanced readability). The survey was designed to be self-explanatory, and contained a description of PAL and a short questionnaire. The description had been validated prior to the study to ensure that it would be pertinent and sufficient. When possible, the investigator explained PAL verbally, and optionally showed the working application, if requested by the participant. We chose not to operate PAL during the study on ethical grounds and to avoid contentious situations. The left side was filled out by the researcher while the participant was filling out his or her part.



Date: 11 / 08 / 04

1) What were you doing / talking about?

Work- some interviews w/car dealers

2) Sensitive information involved

No   Financial   Health   [✓ Other]

Proprietary

3) Physical location

at work near one another

4) Number of people around at microphone reach

1 + me

5) Notes (include your relationship with the person)

Co-worker

0216

The Personal Audio Loop

The Personal Audio Loop (PAL) continuously records sound and voices from the user's environment. The device allows the user to replay, at any specific moment in time, any sound that was heard in the recent past, up to a defined maximum time span (for example, up to 1 hour in the past). Sound older than that is automatically erased and cannot be replayed. Currently, PAL is integrated in a cell phone (see figure), but the device only records sound from the environment, and not phone conversations. The user can replay the recording and rewind and fast forward through it. The stored audio can be heard either through the loudspeaker on the phone, or through the external speaker/mike.

People who used this device, employed it as a memory aid, as a reminder tool, as a short-term voice notepad and to relay information from one person to another. Although PAL could be useful to many people, we are also aware that other people might have concerns about the privacy of their conversations.

Suppose that the person who gave you this survey is using PAL. We would like to know your opinion about PAL. Please complete the survey on both sides of the card, as soon as possible.

1) How important would it be that she had told you **before** starting the conversation that PAL is running?	Does not matter	Matters very much
	1 2 3 [✓ 4] 5	
2) How important would it be that she had asked for your permission to use PAL?	Not important	Very important
	1 2 [✓ 3] 4 5	
3) For how long after the end of your conversation do you think should PAL store the conversation?	□ as long as he needs ☒ at most one week □ at most one day □ at most one hour □ at most 10 minutes □ I do not know	
4) How likely would it be that you ask her to erase the recording of the conversation you just had?	Not likely	Very likely
	1 [✓ 2] 3 4 5	
5) How important is it that she asks for your permission to copy the conversation to a tape?	Not important	Very important
	1 2 3 4 [✓ 5]	
6) How important is it that she asks for your permission to play the recorded conversation to someone else?	Not important	Very important
	1 2 3 4 [✓ 5]	
7) Do you consider the conversation you were conducting with her confidential?	Not confidential	Very confidential
	[✓ 1] 2 3 4 5	

8) Your Age Range: □ 18-29 □ 30's □ 40's ☒ 50's □ 60 or over

9) Your Sex: □ M ☒ F

10) Your Occupation: media producer

11) Today's date: 11 / 8 / 04

turn card

0216

Figure 6.2: Proxy Study Survey.

The participant was asked to fill out the survey immediately if possible, to increase recall accuracy. Otherwise, the survey portion of the card (lower right in Figure 2) was return-addressed on the backside and could be mailed back at the participant's convenience (we affixed a postage stamp for this purpose). The questionnaire included six questions on a 5-point scale, one multiple-choice question and, on the backside, a blank space for optional comments in addition to our lab's address and space for postage. The questions included the following:

- the importance of being informed about the application;
- the importance of asking permission before using the application;
- the time span for which the subject would allow the user to store the conversation;
- the likelihood that the subject would ask the user to erase the recording;
- the importance of asking for permission to copy and replay the conversation to others; and
- an indication of the subjective "confidentiality" of the conversation.

The survey also included three anonymous demographic questions: age range (in decade), gender and occupation. This structure minimized completion time and, in fact, most participants were able to complete the survey immediately.

I believe that this setup allowed us to gather observations that would have been difficult to obtain with a typical survey or in a laboratory setup. For example, I could have used scenarios to evaluate PAL, asking people to read a short story of one instance of use of PAL and then answer to a survey. However, such a setup would have three drawbacks: 1) it would require participants to reflect on a situation that may not be part of their way of behaving; 2) the selection of the situation and the way the scenario is presented may affect the results; and 3) it would be difficult to create a set of scenarios representative of all possible conversational situations.

Because the paratype combines event-contingent experience sampling with experience prototyping, it is especially useful for evaluating high-level or implicit interaction where reference to concrete instances of life is needed. This is particularly important when we do not know how often these instances arise, or how to describe them (*e.g.*, how often are people in a "confidential" conversation?) and when later recollection of these instances may be inaccurate. The latter may occur when reference is sought to privacy, or, more generally, to social relations, personal preferences, or when considering situated action [161].

In fact, paratypes, and more generally experience sampling, may be useful for gathering early feedback on mobile and ubiquitous technologies, such as applications that collect information at unexpected times (*e.g.*, Microsoft's SenseCam [75]), or provide information when needed (*e.g.*, portable guides), or where interaction is embedded in unplanned social practice or everyday routine, such as home communication systems [133]. These applications may have high prototyping costs; probing salient aspects of the experience without the need for working artifacts may represent an efficient way of obtaining relevant information needed for design.

6.2.2 Caveats

When using paratypes (and generally mixed experience prototyping and sampling techniques), several issues must be considered, including potential sources of bias related to the people who are used in the sampling and the type of experiences manufactured. Moreover, study implementation cost may be higher than normal surveys.

The demographics of the proxies are likely to influence the demographics of the respondents, in terms of age, socio-economic class, education, *etc.* In the PAL Proxy study, the proxies' age, profession and social class are reflected in the respondents'. Also, relative differences in age, gender and socio-economic class between proxy and respondent could influence the results. To control these variables, it is advisable to recruit a diverse group of proxies as possible, and to verify that their social interaction patterns actually reach the target demographic by using exercises specifically developed for this purpose [129].

Selection bias on the probed situations may also represent a potential issue with paratypes and experience sampling. Research ethics and social appropriateness may suggest avoiding intrusive studies in sensitive situations (*e.g.*, at a funeral) and to resort to more hypothetical means for probing behavior. Certain countermeasures may decrease or control situation selection bias. First, the researcher administering the survey could complete only his side of the data, without handing out the survey to the participant. This would provide a statistic on the number of situations that were not probed, and the reason why this did not happen, thus allowing researchers to plan supplemental inquiry. Second, administration of the experience sampling survey could be deferred to a more appropriate moment. Researcher's notes could be used to help the participant recollect the situation, although there is a risk of introducing even more bias.

While conducting an experience sampling study is decidedly less expensive than a deployment with a working prototype, which typically has high development, recruitment, and operational costs, it is not, by any means, a 'discount usability' technique [135]. It still requires careful planning and its execution is more complex than a mass survey administered via email or by stopping people in a shopping mall. Cost is related to sample size. The number of participants of ESM studies (and of our PAL Proxy study) is generally low compared to other privacy surveys such as the GVU WWW User Surveys [83] and Ackerman *et al.*'s e-commerce surveys mentioned above [15]. In effect, experience sampling trades quantity for increased authenticity and *situatedness*. Given the lower number of participants it is especially important to verify demographic coverage when using these techniques.

Disruption is an important consideration as well. Because immediate feedback is sought, the survey must fit within the timeframe of the interaction that it is probing. The PAL Proxy study succeeded in this, although at the cost of having to sensibly cut down the number of questions asked. One practical problem we incurred in this respect was related to consent requirements set by our IRB (Institutional Review Board). Although we did not have to document participants' consent (*i.e.*, have them sign a consent form), we still had to provide them with an information notice. Reading the one-and-a-half page notice disrupted the experience even further than the disruption caused by filling out the survey. More concise consent notices would be helpful, though changing standard wording requires extensive collaboration with IRB officials.

6.3 Using Prototypes in Deployments with Users

While Experience Sampling can be used to gain early feedback on ubicomp technologies with reduced cost, developing prototypes and deploying them with test users can prove to be a much more costly endeavor. The advantage, however, is increased realism, leading to supposedly more reliable data, and the ability to identify emergent issues.

The deployment of the Reno application that I conducted with Intel Research, mentioned in Chapter 4, is an example of such a study done to answer specific privacy questions. Colleagues at Intel had previously focused on the privacy implications of disclosing the user's location (Consolvo *et al.*'s ESM study) and at understanding usage (Smith *et al.*'s pilot deployment). The deployment I carried out with two families with teenage children investigated the issues of plausible deniability and the need for automatic functions within the application [99, 100]. In this study we used a number of instruments to gather data: usage was logged on the phone and reported back to the researchers once a day using SMS and emails. We interviewed the participants twice, after sending them email questionnaires every other day. And we collected demographic and preference data using questionnaires.

The results of the interviews were interesting because they showed that privacy was subsumed in a broader system of concerns and requirements. For example, Reno could be configured to reply automatically to location requests (the Instant Reply function described in Section 4.3.2.1), but participants did not use this automatic feature. We expected privacy to be the primary reason. Instead, interview records show that the primary reasons were a lack of need, the desire to avoid misleading their conversation partners with potentially wrong disclosures and to maintain expressive control on the communication; achieving privacy protection and maintaining the freedom to exercise plausible deniability was mentioned only occasionally by participants [99].

In that study, one-to-one interviews proved to be good investigative tools for understanding the *intent* of individuals' actions with relation to privacy. Even then, it is important to separate causes and effects carefully. The Reno study was focused on privacy, but we were careful not to address the issue of privacy upfront in the interviews, in order to avoid biasing participants. We addressed the issue of privacy explicitly only at the end of the last interview, if the participant had not brought it up autonomously. Had we sought explicit feedback on privacy upfront, we may have obtained skewed observations, in terms of an excessive focus on privacy. Focusing on utility and day-to-day management instead, allowed us to frame privacy questions in broader terms that I believe are more representative of potential use.

In contrast, log data on the use of the application proved difficult to interpret in isolation, and we did not succeed in gathering statistic data on the reasons for using the application, notwithstanding the email questionnaires sent every other day to sample use contained questions about use purpose. One of the reasons for this was that the deployment was too short and usage did not settle. This invalidated claims that our observations would be representative of actual long-term use. Furthermore, we did not collect descriptive information about enough instances of use from the users in the interviews (*e.g.*, explanations why they sent a particular message). For these reasons we chose not to use the traffic logs to derive conclusions on privacy and security, and resorted mostly on qualitative data from interviews instead.

The Reno study highlighted some potential issues that must be considered when performing this type of deployment to probe privacy and security, including the characterization of users, learning curves and deployment circumstances. These issues are discussed in further detail below.

6.3.1 User Characterization

One issue is how to characterize users and their need for security and privacy features. Attributing needs for specific security features to certain user groups based on common sense can be very misleading. In the Reno deployment, with the support of social psychology literature and common sense, we assumed that deceptive practices among teens and parents would be quite prominent. When we failed to observe the amount of deception we had hypothesized, we were forced to look back and reconsider our assumptions. First, we observed large variability among teens in their use of the technology. Each user appropriated the system in different ways, and each teenager had different privacy needs which required different security strategies. For example, one participant formed a very clear mental model of the application and demonstrated the ability to actively deceive his parents about his location in order to achieve personal privacy with regard to the places he desired to go. This participant admitted that he would have never voluntarily used the Instant Reply feature, because he worried that his parents would have used it as a surveillance tool to prevent him visiting certain friends. If forced, he also claimed that he would label places in a way that would not cause repercussions with his parents.

Some participants relied on their parents providing transportation to achieve their own social goals and thus were quite insensitive to privacy concerns. Other teenagers thought that socially induced self-restraint would have prevented abuse of the automatic reply function (*e.g.*, stalking), because the requesting party's identity would have be visible in their Reno inbox.

Thus, characterizing use of privacy and security features based on broad social groups like ‘parents’ and ‘teens’ was demonstrated to be exceedingly blunt. Characterization must be more fine-grained to provide high quality results, especially in studies with small participant pools.

6.3.2 Long Learning Curves

User studies that target the security and privacy-related features of applications are hampered by the fact that these features, deriving from non-functional requirements, tend to remain invisible until users really need them or some incident occurs. This mundane observation has the consequence that it is difficult to define the length of a user study that reliably produces observations on the use of such features.

We found that the Reno application was not fully appropriated even after 14 days of deployment. (The application was running, in the average across participants, 48% of the total study time, thus for the majority of the wake hours). Reno was arguably a simple application composed of 40–50 interaction steps (screens) accessible to the user (approx. 15,600 lines of Java code). Considerable effort went into fine-tuning the interface, which had been reviewed after the pilot study, and subjected to a cognitive walkthrough by two experienced HCI professionals. Notwithstanding training and access to detailed documentation, most participants took one full week to become acquainted with the application’s basic functionality, and a majority of participants never used advanced features with security implications such as the automatic features and the auditing functions.

Longer studies may allow researchers to observe the usage of these technologies, but cost concerns may limit the duration of deployment studies. However, in the Reno study, most of the cost was incurred during the planning and development phases, and not during the actual deployment. On the other hand, long deployments may be problematic for recruitment, requiring higher compensations and incurring higher recruitment costs. Long deployments also require guarantees against usability issues or malfunctions in the software, or contingency plans in the event issues should arise. Segmented deployments may provide the best results. In these deployments, participants use the application for a certain amount of time. The application is then fine-tuned, and showstopper bugs are fixed. The same set of participants then use the application again for the remainder of the study, which reduces deployment costs related to learning.

6.3.3 The Impact of Deployment Circumstances

As people's social activity and practices vary not only over the course of a life-span but in yearly, weekly and shorter cycles, the results of user studies can be strongly influenced by the specific circumstances of a deployment. This demands careful selection of appropriate times of year for performing specific studies. In the Reno deployment study, for example, it was observed that the tight schedules of most teens, and the time of year, during school, just before major holidays, reduced their independent mobility. I believe this impacted our observation of deceptive practices both between peers, and with their parents.

Some participants went as far as spontaneously noting that repeating the study during the summer vacation could have produced very different usage patterns. During that time, teen participants would have been much more mobile and independent than during the period of our deployment, and potential deceptive practices related to their specific activities outside of the home may have been very different. Again, this issue emphasizes the latent character of security and privacy requirements.

6.4 Looking at Both Sides of the Issue

The proportionality method suggests that designers should examine both the benefits that an application provides to the user and the security and privacy constraints of all affected parties. For example, in the PAL application, we considered both the primary user's needs and his or her conversation partners' concerns, as well as the concerns of other third parties. In some cases, a trade-off among design choices can be reached. One fundamental parameter of the application is the retention time of the buffer—proportionality suggested a balance between a useful enough application and a minimal invasion of privacy.

Application usefulness was probed using a diary study. In that study, participants were asked to complete a very short survey about when they would like to use PAL to recall previously recorded audio. These surveys were collected in a diary that participants carried with them (Figure 6.1). One of the questions asked how long ago the experience of interest occurred. With this question, we wanted to understand how long the buffer would have to be in order for the application to be useful. Study results suggested to fix this time between 15 and 60 minutes, because participants estimated that a majority of events had occurred less than 60 minutes prior to the moment when the user wanted to recall them. This seemed to us a very reasonable retention time in order to minimize risk. We then probed in the Proxy study the symmetric opinion, *i.e.*, the conversation partner's take on how long they would allow the user to retain the conversation. We were surprised when they indicated much longer retention times than we had initially hypothesized.

In Chapter 4, I pointed out that the 'balancing' between stakeholders' needs in terms of privacy *vs.* usefulness rarely translates into a simple quantitative assessment. An excellent example is provided by the retention time discussion above: at the end of the Proxy study, we concluded that conversation partners were much more concerned about potential *misuse* of the recording than about *retention time*—shifting our initial design question away from a quantitative assessment of retention time and towards preventing misuse. Summarizing, the purpose of the proportionality method is not that of necessarily reaching quantitative balances, but rather that of situating the engineering of privacy and security needs within the broader picture of requirements and stakeholders in the design space.

One interesting question when evaluating both sides of a privacy problem relates to the structure of participants' involvement. One way to structure a study is to ask questions about usefulness and privacy concerns to different participants. A second approach would be that of asking both questions to the same participant. For example, Consolvo *et al.* attempted to probe both sides of a location disclosure in the ESM study of Reno [51]. The participants were asked to indicate their availability to disclosing their location at fictitious requests generated randomly by a handheld device they carried with them. Occasionally, a final question on the survey also asked them to indicate whether they would have wanted to know the requesting party's location as well. Considering the need to reference instances of real life, discussed in Section 6.2, this final question, which relates to the usefulness of the person finder, appears even more detached from everyday needs than the random location request. Not surprisingly, the authors de-emphasized the results of that part of the survey, concentrating on privacy instead.

However, probing both sides of the disclosure with the same participant may affect his or her responses. In particular, participants may be led to understanding the utility of the application and perhaps the potential for misuse, which might provide an advantage in evaluating the risks related to the privacy issues. Similarly, in the Reno deployment study, participants used the application both for requesting and disclosing their location, because the application was *symmetric*. In the PAL case, instead, two separate studies were performed to understand the two sides of the issue. One concern with this setup is that the participants of the Proxy study would have been overly exposed to the negative impact of the application. For this reason, in the PAL description in the Proxy study (reported in Appendix B), we attempted to provide a neutral description of the application, mentioning both the usefulness of the application and the potential risks. Clearly, this is a tricky manipulation, due to the risk of biasing the results. I attempted to hedged against biasing the description by conducting multiple expert reviews of the descriptive text.

6.5 Design Guidelines, Design Methods and Analytic Tools

Throughout this thesis, I argued that uncharted fields such as ubicomp privacy and security may be best tackled using *generative* frameworks rather than prescriptive techniques such as privacy guidelines. By generative, I mean frameworks that help identify (generate) design questions as opposed to prescribing solutions. The proportionality method and the advocacy of employing UCD techniques embody this conviction. I claimed that privacy guidelines, such as those proposed by Langheinrich [116] represent a useful starting point but may be too vague to provide detailed guidance for many applications whose purpose, utility and impact on the security and privacy of stakeholders are unclear.

While in general I stand by this viewpoint, prescriptive guidelines still have a role in ubicomp design. Following the Reno deployment, I wrote, with the other researchers involved in that project, a summary article of the entire application evaluation and design cycle (the ESM study, the pilot and the deployment). In that paper, entitled *Developing Privacy Guidelines for Social Location Disclosure Applications and Services*, I proposed a set of eight guidelines for the development of social location disclosure applications [100], shown in Figure 6.3. These guidelines specifically highlight privacy concerns in social location disclosure applications and in the paper it was argued that they were necessary but not sufficient for achieving a successful design.

Applying design guidelines has been traditionally problematic in the mobile and ubiquitous computing field, which suffers from the lack of an established design practice. In the paper mentioned above, I applied these guidelines to an evolution of Reno, to demonstrate how they can inform the development of a new applications. I indicated where the guidelines came into play in the new design, both as justifications for design choices, or as warnings that design choices made for satisfying other needs (such as supporting group communication) might cause acceptance problems.

Flexible Replies.

Support Denial.

Support Simple Evasion (*e.g.*, “I’m busy”).

Don’t Start With Automation.

Support Deception.

Start with Person to Person Communication.

Provide Status / Away Messages.

Operators Should Avoid Handling User Data.

Figure 6.3: Privacy Guidelines for Social Location Disclosure Applications and Services.

Guidelines focused on one type of application may be easier to apply reliably, because similar design problems may have similar solutions. In the case of Reno and its evolution the difference was relatively minor. By contrast, in Chung *et al.*’s evaluation of design patterns, the difference between the application that was being designed and the examples encoded by the design patterns was significant and this may have been one of the reasons for the failure of that experiment. Their patterns were also expressed at a very high level, perhaps too high to be used effectively (see Table 3.2). In Chapter 5, I make a similar observation, claiming that Bellotti and Sellen’s Feedback / Control framework may not provide guidance for applications that are different from video media spaces (*e.g.*, mobile applications).

The discussion above suggests that there is no straightforward answer to what design techniques or methods are most effective in this domain. The lack of success of prescriptive guidelines may be due to their misapplication more than to their lack of value. The various techniques and methods presented in this thesis may provide an advantage to designers in specific situations. An interesting question then is at what point, in the design cycle of ubiquitous computing applications, are the various design techniques discussed here best employed? The answer to this question assumes, perhaps a bit improperly, that it is possible to generalize the findings of this thesis, but I believe it is a worthy research question that should be asked. Rather than providing a conclusive answer to this question, in the following, final Chapter, I will frame the discussion as suggestions that may be considered for future research.

CHAPTER 7

TOWARDS AN INTEGRATED APPROACH

Viewing the proportionality method as a scaffold suggests a metaphor useful for answering the question posed at the end of the previous chapter: What role do different design techniques and methods play in this problem domain and when should we apply them? Generative design methods could provide the structure of the analysis tasks facing the designer; the voids in the structure could then be 'filled out' using specific tools and techniques. In the Reno and PAL case studies, I used the proportionality method to frame the basic application questions, and to connect questions about privacy and security to the general requirements of the application. Various types of inquiry techniques were then employed to obtain answers to relevant privacy and security questions, including diary studies, experience sampling, deployments, legal analysis, bibliographic analysis, and the application of design guidelines.

7.1 The Role of General Design Methods

The comparison between design methods documented in Chapter 5 suggests that in that experiment, participants' use of different methods did not relate to significant quantitative performance differences in two important metrics—identified issues and the complexity of the resulting design. However, the four methods made a difference in how participants approached the design task they were assigned. The differences are both formal and related to content. The formal differences consist in the structure of the design deliverables, in the type of external resources (*e.g.*, reference literature) that participants used, and in the order in which design determinations were made. Although I did not collect statistical data on these effects, I believe that they had an impact on the overall conclusions of a design process. The content-related differences refer to the types of questions that were asked by the participants. As suggested by the Issue Type analysis in Section 5.2.5.4 (page 163), each design method highlighted certain concerns, risks or issues, mostly as a result of the specific ‘checklists’ they propose to the designer.

Based on these observations, one may conclude that the role of a generative design method is that of gaining broad coverage of the design space, by generating as many *questions* and issues upfront and reducing the time necessary for gaining a broad understanding of the design space structure. In this respect, the Risk Analysis phase of Hong *et al.*’s method and the Proportionality method appeared to fare better than the other two conditions in the evaluation study, because they produced a higher number of unique issues and a wider spectrum of issue types. These questions can then be used to bootstrap further research or design decisions. This characterization matches what is commonly associated with ‘second-generation’ design methods in the design method research community [63].

Given that none of the methods tested in the evaluation study reached the full set of security and privacy issues (Figure 5.10 on page 162), it follows that there is still a research opportunity in compiling more exhaustive check-lists or generative methods that allow designers to reach broader coverage, or at least better characterizing generative methods in terms of the type of applications they target. One way of proceeding, based on evidence in Table 5.12 would be that of combining a general design method (*e.g.*, Risk Analysis, Proportionality) with specific guidelines covering aspects of the design space (*e.g.*, Bellotti and Sellen’s Feedback / Control, my Design Guidelines for Social Location Disclosure Applications, and security management guidelines).

7.2 The Role of User Studies

Once general issues have been identified, prescriptive methods can provide local design guidance. As noted above, however, these guidelines should not be applied before understanding the broader issues involved in the application’s design. For this purpose, some type of real-world evaluation of the application concept may be necessary. User studies may be useful in this context, but are often perceived as overly costly, especially if performed uniquely for investigating non-functional aspects of design such as privacy and security. For this reason, reference to existing bibliography for meeting reasoned design choices may be a cheaper alternative—legislation, market research, ethnographic research. Piggybacking on other formative studies being conducted for other purposes may be possible, too.

User studies, especially targeted at what Wynekoop and Conger [183] call "research for understanding,"[56] also represent valuable generative techniques for identifying privacy and security issues. This is especially true for studies that reference working technology in realistic settings, such as deployments and field studies (consider, for example, the insights we gathered through the PAL Proxy and Reno deployment studies). Clearly, user studies are employed in HCI practice for summative purposes as well, but such use is less relevant to the topic of this thesis.

A growing number of researchers targeted privacy and security in the past few years, and this very thesis attempts to contribute to the state of the art of the development of user study techniques in this domain. However, there is still much work to be done in this area. Interesting research questions include understanding which user study techniques are most appropriate for investigating specific privacy and security questions, users and applications. Furthermore, it would be interesting to assess the optimal cost-benefit for this kind of studies, in order to increase their efficiency.

[56] That is, "research focusing on finding the meaning of studied phenomena through *e.g.* frameworks or theories developed from collected data." [183] Wynekoop and Conger published a classification of research paper types in 1990, with reference to the Software Engineering community. Their model was subsequently adopted by Kjeldskov and Graham [112] who analyzed publications in the Mobile HCI community.

7.3 The Role of Specific Guidelines and Analytic Frameworks

Design guidelines are prescriptive methods, *i.e.*, methods that provide a solution or an indication on how to solve a specific problem. Examples of prescriptive methods in this domain include the design guidelines derived by Langheinrich from the FIPS [116], or those generated from evaluation of case studies [45, 100]. They are popular due to their relatively simple structure and ease-of-use.

Analytic frameworks may be seen as an evolution of prescriptive guidelines. One of the most well-known analytic framework in this domain is the Approximate Information Flows framework. AIF provides both design guidelines (*i.e.*, reduce information asymmetry) and a way to describe privacy management as a set of data exchanges and manipulations [110]. It further suggests constraints on these manipulations in order to achieve privacy goals. This thesis did not consider analytic frameworks explicitly. However, the prescriptive nature of these frameworks suggests that they should be employed similarly to other prescriptive guidelines, after basic knowledge about the application, the social context and the user purposes has been acquired. One important caveat in the use of prescriptive methods is the scope of applicability of these methods. Guidelines developed from experience in one application domain may be, in the best case, difficult to apply to other domains, as suggested by the relatively low number of unique design issues identified by participants in that condition (see Table 5.11 on page 159). In the worst case, they may mislead designers towards irrelevant issues and detrimental design choices. In particular, methods developed for addressing personal privacy should not be employed for solving data protection concerns, as the design solutions are in some cases opposite.

One interesting research question would be to evaluate analytic frameworks and guidelines both in terms of their expressive potential and with relation to the design conclusions they lead to. This could be done by extending the analysis of Section 5.2.5.3 on page 159, in the style of how Nielsen evaluated the effectiveness of general heuristic techniques, or Mankoff *et al.*'s evaluation of ambient displays heuristics [125].

7.4 Completeness and Documentation

Completeness of the analysis of the design space is a classic problem in all exploratory design disciplines. The proportionality method is essentially a heuristic design method, which puts it at odds with structured SE processes targeted at achieving high assurance of exhausting the analysis and design space. Within the proportionality method, assurance may be provided, if at all, by the thoroughness of the analysis of the questions indicated by the design method. I do not address the issue of completeness in this thesis, and merely suggest standard workarounds (*e.g.*, using multiple designers, cyclic design processes, *etc.*). It should be noted, however, that some of these workarounds assume that enough prior experience is available—a questionable assumption in the undeveloped field of ubicomp.

A practical concern related to completeness in SE is that of producing adequate process documentation.[57] Not only is documentation essential for preserving memory of a specific application development process, but it also constitutes the main product and communication tool within design groups. When I initially started working on this design method, I did not consider the issue of documentation, because I assumed that the intermediate and final products of the design method would be relatively short and self-contained. After the experience of the first two case studies, it appears that this assumption may not hold as the systems under consideration expand in complexity. While the PAL application described in Chapter 4 could be designed without a formal documentation process, other systems may require a more formal documentation format associated

[57] K. Rannenberg, personal correspondence.

with the proportionality method. In Chapter 3, two approaches to the documentation problem were cited: Design Rationale and formal Protection Profiles [105].

The proponents of Design Rationale express the common opinion that managing complex designs requires the ability to trace design choices back to the motivating factors or requirements [124]. Design Rationale was used in the evaluation study as the control condition and I did not observe significant differences in the size of the design deliverable. Anecdotal observation suggests that participants using Design Rationale connected privacy and security issues more explicitly to design choices, but that the overall quality of the deliverable, as evaluated by the independent reviewers, was not affected by this. Providing a design rationale may not have been considered an advantage by the evaluators in that context. In fact, the overall quality of the deliverables documentation, as expressed by the clarity score (*EL*) by the two evaluators was *lowest* in the Risk Analysis and Design Rationale conditions. This suggests that the documentation format suggested by Design Rationale may be not be sufficient to provide adequate documentation for this type of design problems.

Formal documentation proposed by established SE standards such as the Common Criteria may provide higher assurance of requirements coverage and rationale connections, but does so at a very high cost that may be premature for many research ubicomp applications. What is lacking in traditional documentation formats such as Design Rationale and Common Criteria is the ability to keep track of post-deployment events. If learning from experience is the goal, proper documentation of such experience is necessary. I believe that an interesting research question related to the domain of this thesis, and, generally, to ubicomp in general, is how to document valuable experience with real applications in a way that can inform design at later stages.

7.5 Novel Technology vs. Evolution

One important aspect of technological development that was not addressed in this work relates to the effectiveness of the proportionality method to handle technological evolution as opposed to original designs.[58] Technology may evolve because users appropriate it in unforeseen ways, or due to gradual repurposing and further development. Technology appropriation by users has long been a topic of research in the IT community, and the proportionality method suggests to investigate the issue of appropriation using adequate user study techniques, prior to, during and after development.

However, the proportionality method is aimed at helping design, so it should be usable both in situations where applications are developed *ex novo*, and in situations where existing systems are expanded to support new applications that can unsettle existing privacy / security assumptions (*e.g.*, the example in Chapter 2 of city-wide surveillance systems). Clearly, using the proportionality method assumes that the desirability and appropriateness questions are worth asking (*i.e.*, the outcome is not obvious and the designer can actually do something about it). This may or not be the case when considering evolutions of existing applications. If the designer's analysis cannot influence development due to constraints inherited from the existing systems, the proportionality method could be at least used similar to how DPAs have employed desirability and appropriateness questions in analyzing existing technology—as a summative analysis tool. This hints at an interesting research opportunity: understanding the role of existing technology's constraints on the privacy and security properties of evolutionary systems.

[58] K. Rannenberg, personal conversation.

7.6 The Notable Absent: Security Management

In Chapter 2, I suggested that security management is notably absent from the research in this field. Participants in the design method evaluation study also ignored management. One reason for this is that the design of post-deployment security management processes is usually not viewed as an integral part of product design. However, this situation is at odds with the needs of industry and users. Lately, both industry and academia are coming to the understanding that without careful planning for management procedures, technological security measures can become at best ineffective, and may even be counterproductive [148].

I believe that more attention to security management in ubicomp is urgent and throughout my doctoral work have attempted to translate this belief in action. One of the objectives of the proportionality method is that of producing, in addition to design guidelines for the product itself, also suggestions on the organizational, policy or other post-deployment measures to address security or privacy risks that the technology cannot, by itself, counter. Furthermore, I have attempted to document a systematic analysis of the management challenges related to security in the ubicomp domain, and of their relationship with design [96].

The results of the design study suggest that all design methods, including the proportionality method, failed to stimulate participants to consider management issues as part of the design of the application. These results may have been influenced in part by the limited available time and by the design brief that suggested to concentrate on the artifact. In the pilot study, where I explicitly asked participants to consider management as well as product design, management issues were cited by participants. However, it is clear that more research is necessary to understand the relationship between design, security management and the use of ubicomp applications.

7.7 Conclusion

The capable designer selects the appropriate tools for solving the problem at hand. The concept of proportionality can be a helpful aid in decomposing complex security and privacy issues where no obvious solution is available. However, the proportionality method does not exclude the methods or techniques suggested by others to tackle the end-user security and privacy issues in ubicomp.

In fact, if a summary conclusion can be drawn from this work, it is that none of the methods proposed to date in this field can be applied unconditionally—doing so may be misleading or even detrimental. I have attempted to indicate to what types of problems certain methods and tools are best applied and the relationship of mutual support existing between the proportionality design method and other methods and guidelines. In this process, the qualitative results of the evaluation study have proven more compelling and informative than the quantitative outcomes. Furthermore, this work shows how different types of research questions (*e.g.*, data protection *vs.* personal privacy concerns, technologies at different levels of maturity) demand different user study and analysis techniques.

Along the way, I identified many interesting research problems, including further investigating the power of generative design methods, the constraints and effectiveness of user study techniques, and the applicability of prescriptive methods. The problem of security management in ubicomp deserves special consideration: not only is research on security management missing, but so are also the methodological tools to conduct such research. Important assumptions typically associated with security management do not hold when considering ubicomp applications—impacting the success metrics and solutions employed in traditional IT security management.

I hope that the reader will appreciate that this thesis shines a light in a deep cave of research problems. Many of these problems are timely, relevant and within reach, making them prime candidates for rich future developments.

APPENDIX A

UBICOMP PRIVACY AND SECURITY RESEARCH VENUES

Tables A.1 and A.2 report a list of conferences and workshops that have published work on topics related to ubicomp security and privacy.

Table A.1: Conferences for Ubicomp Security and Privacy.

Conference Name	**URL**
Ubicomp – International Conference on Ubiquitous Computing	http://www.ubicomp.org
Pervasive – International Conference on Pervasive Computing	http://www.pervasive2006.org/
PerCom – IEEE International Conference on Pervasive Computing and Communications	http://www.percom.org/
Mobisys – International Conference on Mobile Systems, Applications and Services	http://www.sigmobile.org/mobisys/
Mobile HCI – International Conference on Human Computer Interaction with Mobile Devices and Services	http://www.mobilehci.org
Security in Pervasive Computing	http://www.spc-conf.org

Table A.2: Past Workshops for Ubicomp Security and Privacy.

Ubicomp 2002 Workshop on Security in Ubiquitous Computing http://www.teco.edu/~philip/ubicomp2002ws/	
Ubicomp 2003 Workshop Ubicomp communities: privacy as boundary negotiation	http://guir.berkeley.edu/pubs/ubicomp2003/privacy workshop/
Ubicomp 2003 Workshop Security in Ubiquitous Computing	http://www.vs.inf.ethz.ch/events/ubicomp2003sec/
Ubicomp 2004 Workshop Ubicomp Privacy: Current Status and Future Directions	
Ubicomp 2005 Privacy in Context Workshop	http://www.sims.berkeley.edu/~jensg/Ubicomp2005
Pervasive 2004 Workshop SPPC: Security and Privacy in Pervasive Computing	http://www.vs.inf.ethz.ch/events/sppc04/
First IEEE International Workshop on Pervasive Computing and Communication Security (associated with PerCom)	http://www.list.gmu.edu/persec/
Second IEEE International Workshop on Pervasive Computing and Communication Security	http://www.cl.cam.ac.uk/persec-2005/
Third IEEE International Workshop on Pervasive Computing and Communication Security	http://www.cl.cam.ac.uk/persec-2006/
Mobile HCI 2004 Workshop On Location Systems Privacy and Control	http://www.cc.gatech.edu/~giac/mhci04lpws/

APPENDIX B

STUDY MATERIALS

This appendix contains reproductions of some of the study materials used in the various user studies conducted as part of this work.

B.1 PAL Study

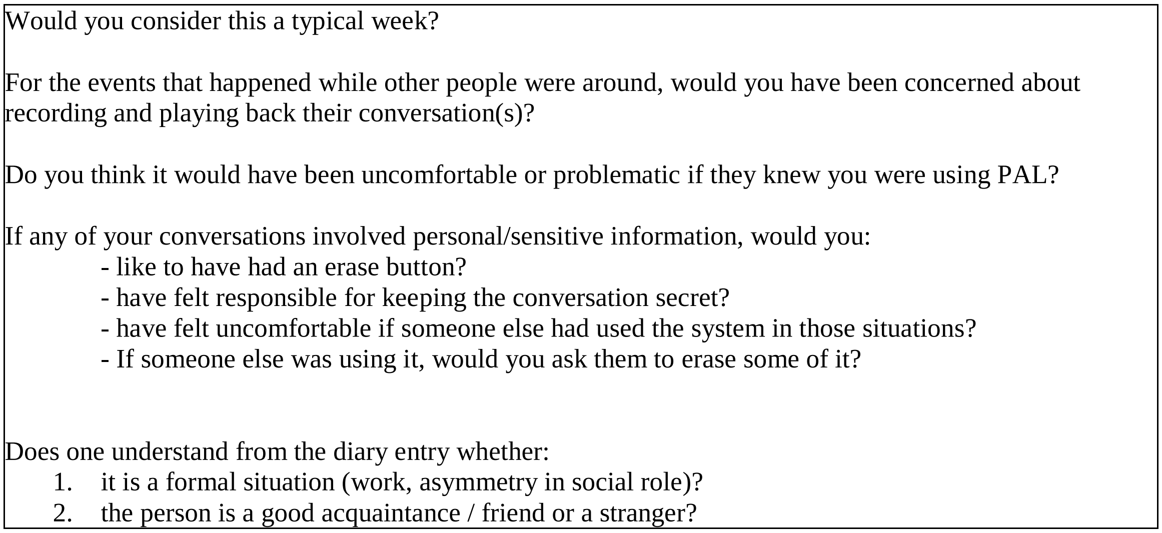
The Personal Audio Loop underwent several user studies, including a lab test of the interface, a diary study, the Proxy study, a short deployment and interviews.

B.1.1 Interview Template

Figures B.1 and B.2 show the PAL diary interview templates. These interviews were conducted at the end of each week during the study. Note how questions about privacy, purposefulness and politeness are mixed in one interview.

B.1.2 Proxy Study

The descriptive text of the PAL Proxy study survey is reported in Figure B.3. (Figure 6.2 depicts the actual format of the survey). This description underwent thorough review to ensure its comprehensibility, brevity and balance.



Would you consider this a typical week?

For the events that happened while other people were around, would you have been concerned about recording and playing back their conversation(s)?

Do you think it would have been uncomfortable or problematic if they knew you were using PAL?

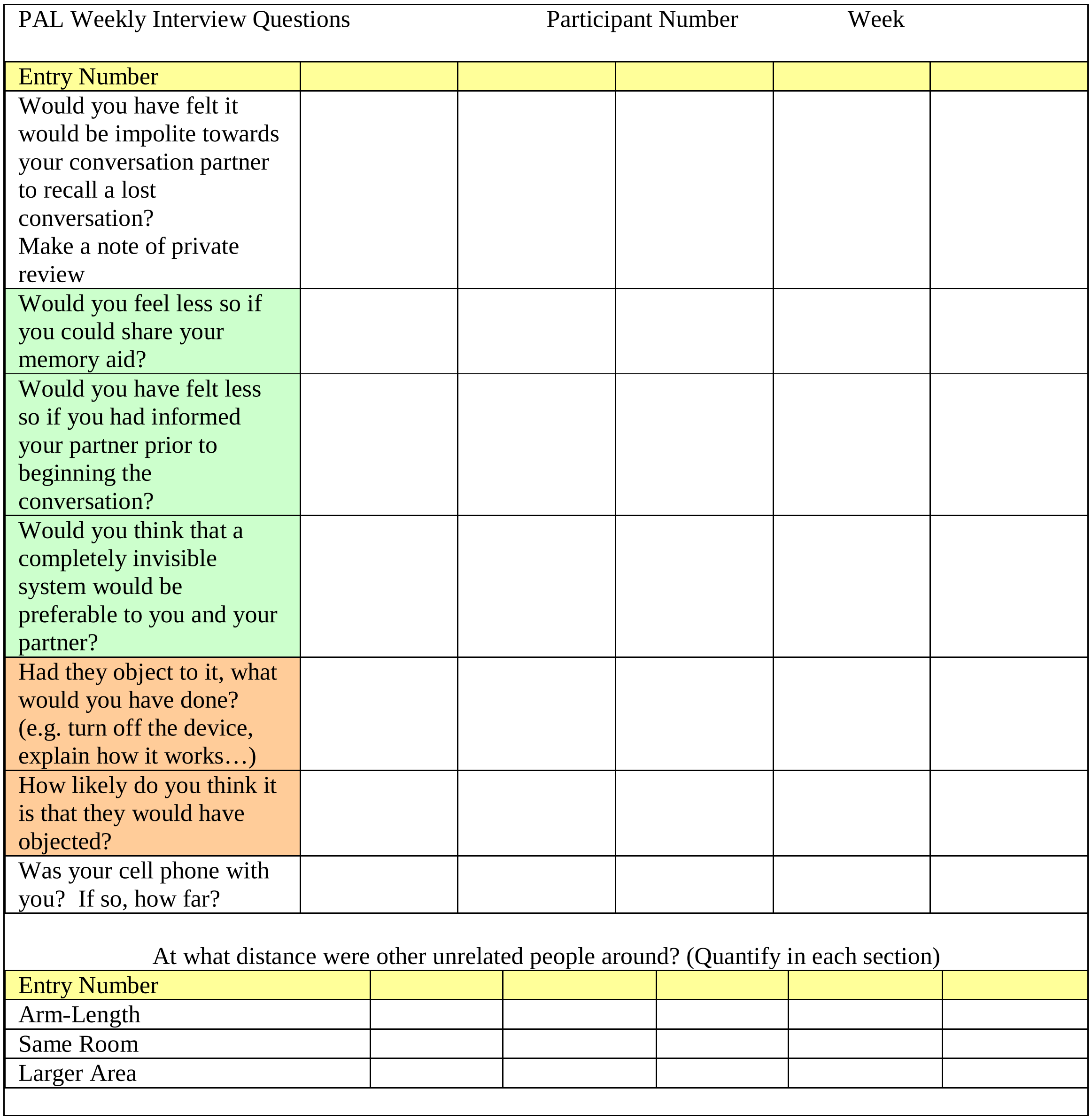
If any of your conversations involved personal/sensitive information, would you:

- like to have had an erase button?
- have felt responsible for keeping the conversation secret?
- have felt uncomfortable if someone else had used the system in those situations?
- If someone else was using it, would you ask them to erase some of it?

Does one understand from the diary entry whether:

1. it is a formal situation (work, asymmetry in social role)?
2. the person is a good acquaintance / friend or a stranger?

Figure B.1: Weekly Interview Template for Diary Study (General Questions).



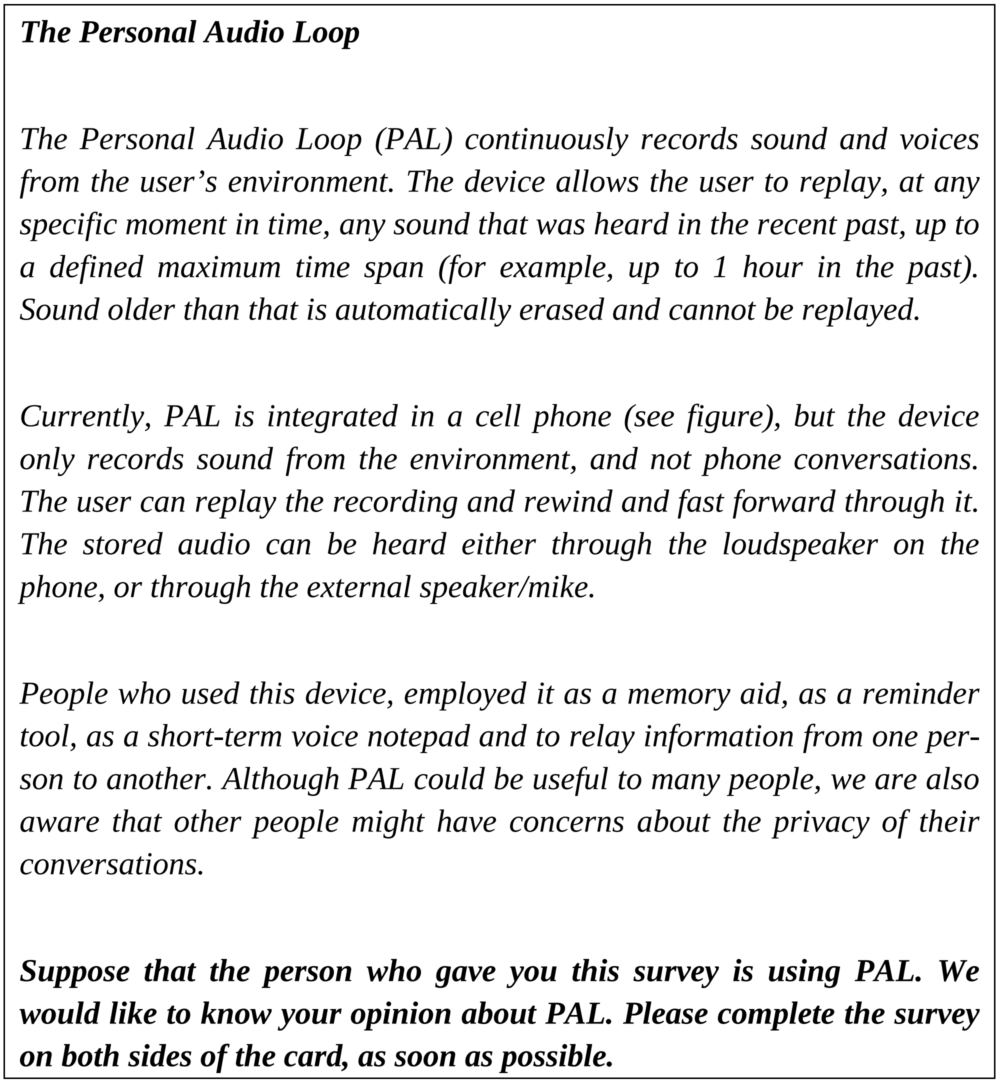
PAL Weekly Interview Questions Participant Number Week

Entry Number					
Would you have felt it would be impolite towards your conversation partner to recall a lost conversation? Make a note of private review					
Would you feel less so if you could share your memory aid?					
Would you have felt less so if you had informed your partner prior to beginning the conversation?					
Would you think that a completely invisible system would be preferable to you and your partner?					
Had they object to it, what would you have done? (e.g. turn off the device, explain how it works…)					
How likely do you think it is that they would have objected?					
Was your cell phone with you? If so, how far?					

At what distance were other unrelated people around? (Quantify in each section)

Entry Number					
Arm-Length					
Same Room					
Larger Area					

Figure B.2: Weekly Interview Template for Diary Study (Event-Specific Questions).



The Personal Audio Loop

The Personal Audio Loop (PAL) continuously records sound and voices from the user’s environment. The device allows the user to replay, at any specific moment in time, any sound that was heard in the recent past, up to a defined maximum time span (for example, up to 1 hour in the past). Sound older than that is automatically erased and cannot be replayed.

Currently, PAL is integrated in a cell phone (see figure), but the device only records sound from the environment, and not phone conversations. The user can replay the recording and rewind and fast forward through it. The stored audio can be heard either through the loudspeaker on the phone, or through the external speaker/mike.

People who used this device, employed it as a memory aid, as a reminder tool, as a short-term voice notepad and to relay information from one person to another. Although PAL could be useful to many people, we are also aware that other people might have concerns about the privacy of their conversations.

Suppose that the person who gave you this survey is using PAL. We would like to know your opinion about PAL. Please complete the survey on both sides of the card, as soon as possible.

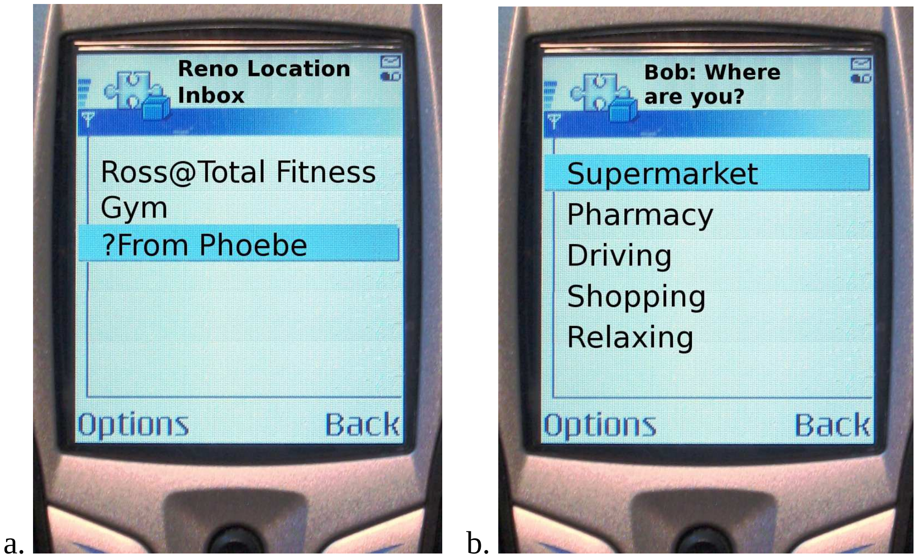
Figure B.3: Descriptive Text on the PAL Proxy Survey.

B.2 Reno Deployment

Figure B.4 shows two screenshots of the Reno application. Reno is modeled according to a messaging metaphor. Incoming location requests and disclosures are displayed on the main screen (Figure B.4.a): the first item is a location disclosure; the second item is a location request by Phoebe. When the user replies to a location request, the application asks to indicate a place name to disclose. Figure B.4.b. shows the selection of a place name. Reno lists places in the physical proximity of the user, as well as activity names.

B.3 Design Method Evaluation Study

Figure B.5 shows the assignment brief given to the Design Method Evaluation study participants. This was provided in electronic form and as a printed sheet in class.



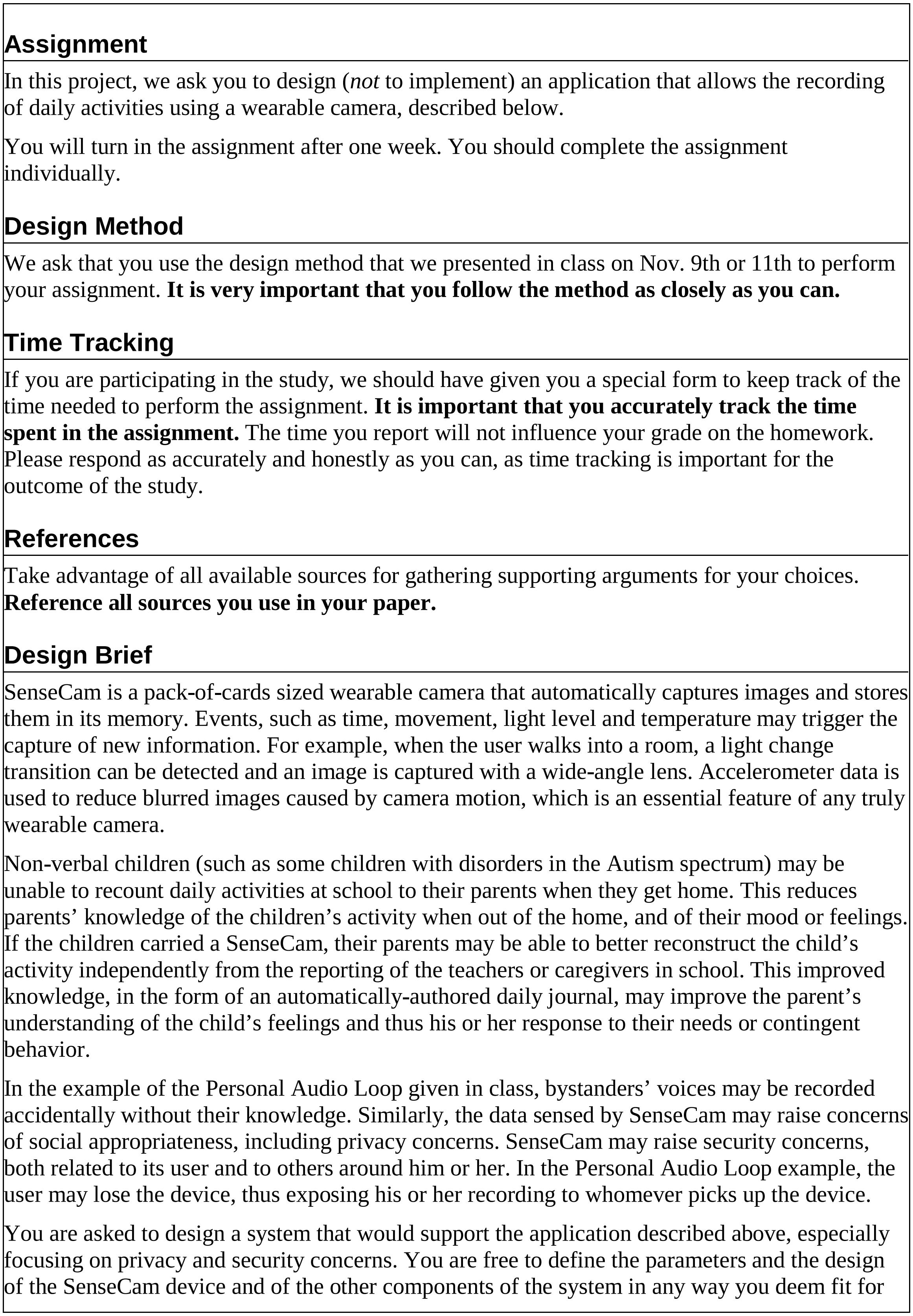
Reno Location Inbox

Ross@Total Fitness Gym

?From Phoebe

Bob: Where are you?

Figure B.4: Reno Screenshots.



Assignment

In this project, we ask you to design (*not* to implement) an application that allows the recording of daily activities using a wearable camera, described below.

You will turn in the assignment after one week. You should complete the assignment individually.

Design Method

We ask that you use the design method that we presented in class on Nov. 9th or 11th to perform your assignment. **It is very important that you follow the method as closely as you can.**

Time Tracking

If you are participating in the study, we should have given you a special form to keep track of the time needed to perform the assignment. **It is important that you accurately track the time spent in the assignment.** The time you report will not influence your grade on the homework. Please respond as accurately and honestly as you can, as time tracking is important for the outcome of the study.

References

Take advantage of all available sources for gathering supporting arguments for your choices. **Reference all sources you use in your paper.**

Design Brief

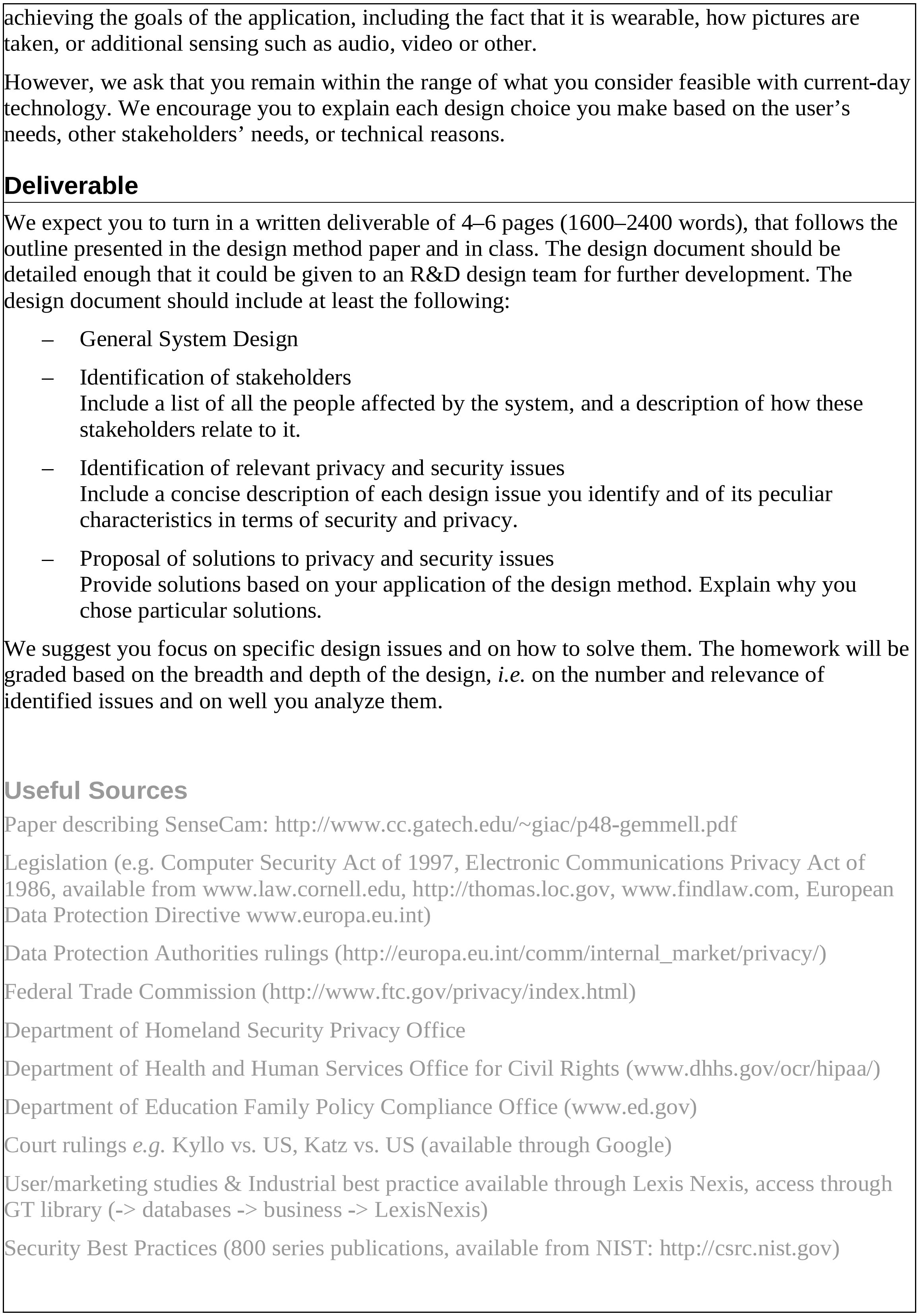
SenseCam is a pack-of-cards sized wearable camera that automatically captures images and stores them in its memory. Events, such as time, movement, light level and temperature may trigger the capture of new information. For example, when the user walks into a room, a light change transition can be detected and an image is captured with a wide-angle lens. Accelerometer data is used to reduce blurred images caused by camera motion, which is an essential feature of any truly wearable camera.

Non-verbal children (such as some children with disorders in the Autism spectrum) may be unable to recount daily activities at school to their parents when they get home. This reduces parents’ knowledge of the children’s activity when out of the home, and of their mood or feelings. If the children carried a SenseCam, their parents may be able to better reconstruct the child’s activity independently from the reporting of the teachers or caregivers in school. This improved knowledge, in the form of an automatically-authored daily journal, may improve the parent’s understanding of the child’s feelings and thus his or her response to their needs or contingent behavior.

In the example of the Personal Audio Loop given in class, bystanders’ voices may be recorded accidentally without their knowledge. Similarly, the data sensed by SenseCam may raise concerns of social appropriateness, including privacy concerns. SenseCam may raise security concerns, both related to its user and to others around him or her. In the Personal Audio Loop example, the user may lose the device, thus exposing his or her recording to whomever picks up the device.

You are asked to design a system that would support the application described above, especially focusing on privacy and security concerns. You are free to define the parameters and the design of the SenseCam device and of the other components of the system in any way you deem fit for

Figure B.5: Assignment for the Design Method Evaluation Study.



achieving the goals of the application, including the fact that it is wearable, how pictures are taken, or additional sensing such as audio, video or other.

However, we ask that you remain within the range of what you consider feasible with current-day technology. We encourage you to explain each design choice you make based on the user's needs, other stakeholders' needs, or technical reasons.

Deliverable

We expect you to turn in a written deliverable of 4–6 pages (1600–2400 words), that follows the outline presented in the design method paper and in class. The design document should be detailed enough that it could be given to an R&D design team for further development. The design document should include at least the following:

- General System Design
- Identification of stakeholders
  Include a list of all the people affected by the system, and a description of how these stakeholders relate to it.
- Identification of relevant privacy and security issues
  Include a concise description of each design issue you identify and of its peculiar characteristics in terms of security and privacy.
- Proposal of solutions to privacy and security issues
  Provide solutions based on your application of the design method. Explain why you chose particular solutions.

We suggest you focus on specific design issues and on how to solve them. The homework will be graded based on the breadth and depth of the design, *i.e.* on the number and relevance of identified issues and on well you analyze them.

Useful Sources

Paper describing SenseCam: http://www.cc.gatech.edu/~giac/p48-gemmell.pdf

Legislation (e.g. Computer Security Act of 1997, Electronic Communications Privacy Act of 1986, available from www.law.cornell.edu, http://thomas.loc.gov, www.findlaw.com, European Data Protection Directive www.europa.eu.int)

Data Protection Authorities rulings (http://europa.eu.int/comm/internal_market/privacy/)

Federal Trade Commission (http://www.ftc.gov/privacy/index.html)

Department of Homeland Security Privacy Office

Department of Health and Human Services Office for Civil Rights (www.dhhs.gov/ocr/hipaa/)

Department of Education Family Policy Compliance Office (www.ed.gov)

Court rulings *e.g.* Kyllo vs. US, Katz vs. US (available through Google)

User/marketing studies & Industrial best practice available through Lexis Nexis, access through GT library (-> databases -> business -> LexisNexis)

Security Best Practices (800 series publications, available from NIST: http://csrc.nist.gov)

Figure B.5: Assignment for the Design Method Evaluation Study. (Continued.)

B.3.1 Adherence Criteria

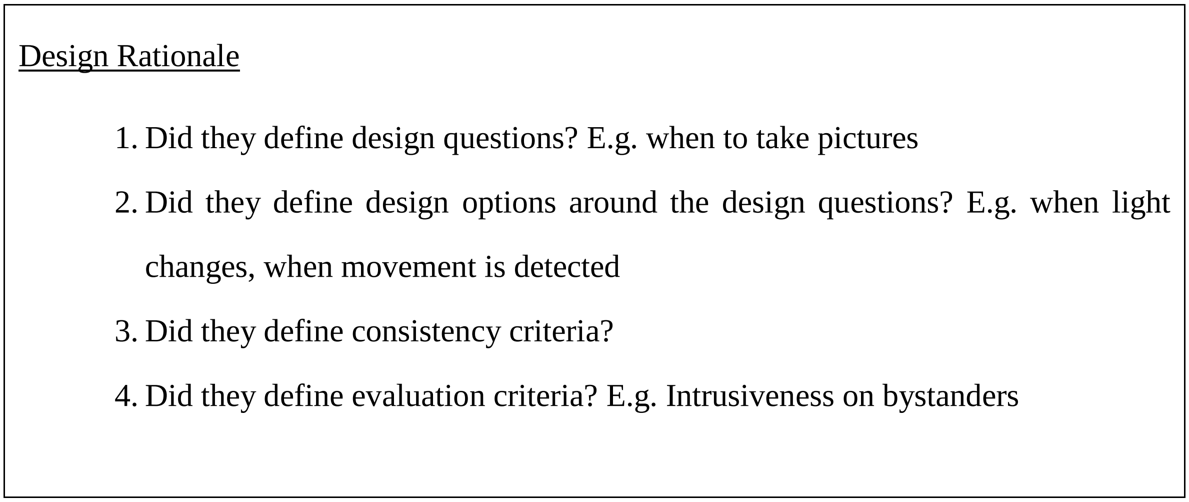
Figure B.6 shows the criteria for the evaluation of the Adherence Score A. The Adherence Score is the proportion of steps the participant followed out of the steps described in the respective design method, according to the lists specified below. For example, if a participant used the risk analysis framework and only followed steps 1–10, the adherence score would be 10 / 17 = 0.59.

B.3.2 Quiz

Figure B.7 shows one of the four quizzes that participants took after completion of the assignment (namely, Bellotti and Sellen’s Feedback / Control method). Each condition had a custom quiz, tailored for their condition.

B.3.3 Lecture Slides

Figure B.8 shows one of the four lecture slide sets (namely, the set used in the Proportionality condition). The other sets differed only in slides 8–16.



Design Rationale

1. Did they define design questions? E.g. when to take pictures
2. Did they define design options around the design questions? E.g. when light changes, when movement is detected
3. Did they define consistency criteria?
4. Did they define evaluation criteria? E.g. Intrusiveness on bystanders

Figure B.6: Adherence Score Calculation Criteria.

Risk Analysis

Identify risks associated with the following questions:

1. Who are the users?

2. What information is shared?

3. What is the value proposition for sharing personal information?

4. Is there potential for malicious data observers?

5. Other Stakeholders?

6. How is information collected?

7. How is information shared?

8. How much information is shared?

9. Qualities of shared information

10.Retention time

11.Prioritizing Risks: Identify L, D C

C = cost of adequate privacy protection

L = likelihood that unwanted disclosure of personal information occurs

D = damage that will happen on such a disclosure

If C < LD do something

Risk management: for at least one identified Risk:

12.How does the unwanted disclosure take place?

13.How much choice, control, and awareness do data sharers have?

14.What are the default settings?

15.In what cases is it easier to prevent unwanted disclosures and abuses?

16.Are there ways for data sharers to maintain plausible deniability?

17.What mechanisms for recourse or recovery are there?

Figure B.6: Adherence Score Calculation Criteria. (Continued.)

Proportionality

Desirability

1. What is the purpose of the application?
2. What are the advantages gained? (e.g., expressed in reduction of risk, or economical benefit)
3. What is the imposed burden? (e.g., in terms of changes of behavior, “chill effect,” or other social costs)

Appropriateness

4. Do the costs and benefits of the selected technology offset the potential invasion of privacy with respect to alternative solutions?
5. Does the technology pose the risk of being abused or employed with further privacy implications?
6. Can the application goals be reached by other means (including non-technical)?

Adequacy —Evaluation of at least one design option according to metrics:

7. What are the characteristics of the privacy-impacting design features?
8. How are design features described as variables?
9. What are the values or ranges of each variable critical to the success of the application?
10. What are the values or ranges of each variable which impact on the privacy of all stakeholders?
11. What compromise is possible between these values or ranges?

Figure B.6: Adherence Score Calculation Criteria. (Continued.)

Did they choose the best design option using the Options/Criteria Table?Feedback/Control

1. Capture: how does the user know what kind of information is being collected?
2. Construction: how does the user know what happens to the information?
3. Accessibility: how does the user know who has access to the information?
4. Purpose: how does the user know how is the information used? …how might it be used in the future?
5. Capture: how can the user control what kind of information is being collected?
6. Construction: how can the user control what happens to the information? Is it stored, processed,…?
7. Accessibility: how can the user control who has access to the information?
8. Purpose: how can the user control how the information is used? …how might it be used in the future?
9. Did they evaluate at least one design solutions based on the following 11 evaluation criteria?

Trustworthiness, Appropriate Timing, Perceptibility, Unobtrusiveness,
Minimal Intrusiveness, Fail-safety, Flexibility, Low-effort,
5. Meaningfulness, Learnability, Low-cost.

Figure B.6: Adherence Score Calculation Criteria. (Continued.)

Ubicomp Privacy Test
Version 1

Name: ______________________________

GT ID: _______________________________

E-Z Pass ® is an automatic toll payment system used on highways in New York, New Jersey and several other States. After subscribing to the system, customers are given a radio transponder to keep in their car that is activated whenever the car drives through a tollbooth, communicating the identity of the customer to the collection system. The toll management company then deducts toll bills automatically from the customer's bank. Each month, customers receive a summary of their transactions.

Bellotti and Sellen propose a structured analysis of ubicomp applications that helps in designing applications with privacy implications. They propose to analyze the collection and use of information in terms of feedback about and control on the information collected about the users.

1. Below, write the what kind of *feedback* the E-Z Pass system should provide to its user about his or her personal information that is collected and used by the system, in the four phases of Capture, Construction, Accessibility and Purposes. Be sure to specify what information about the user you are considering; you should provide one way to provide such feedback at each phase.

    1. Capture

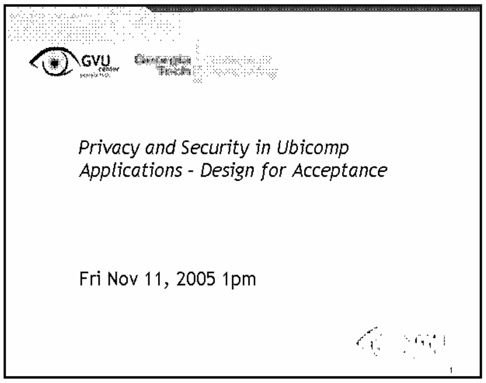
    2. Construction

    3. Accessibility

    4. Purposes

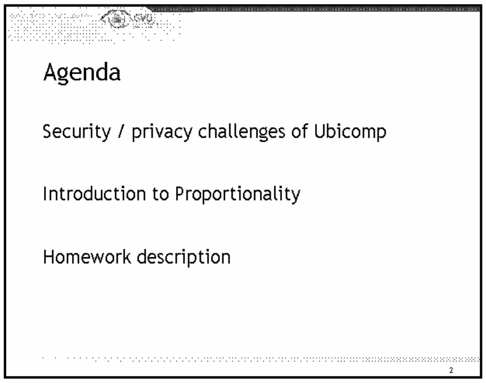
2. Pick any one of the feedback mechanisms you wrote above and evaluate it based on at least two of the 11 *evaluation criteria* proposed by Bellotti and Sellen.

Figure B.7: Sample Quiz for Design Method Evaluation Study.



Privacy and Security in Ubicomp Applications - Design for Acceptance

Fri Nov 11, 2005 1pm

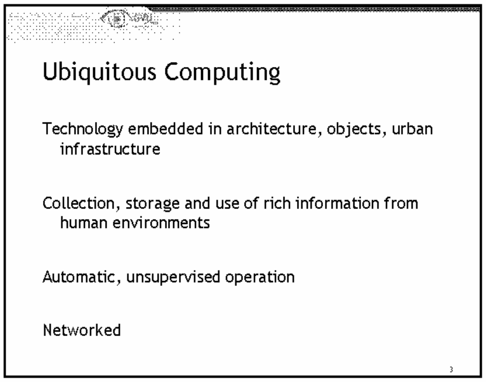


Agenda

Security / privacy challenges of Ubicomp

Introduction to Proportionality

Homework description



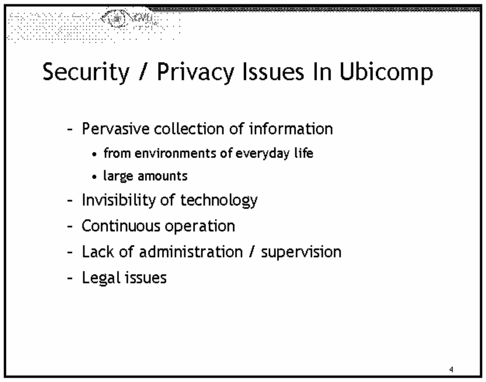
Ubiquitous Computing

Technology embedded in architecture, objects, urban infrastructure

Collection, storage and use of rich information from human environments

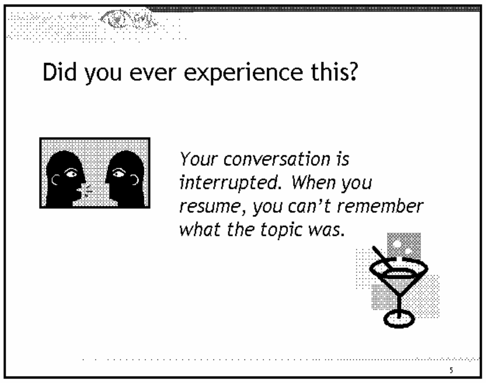
Automatic, unsupervised operation

Networked



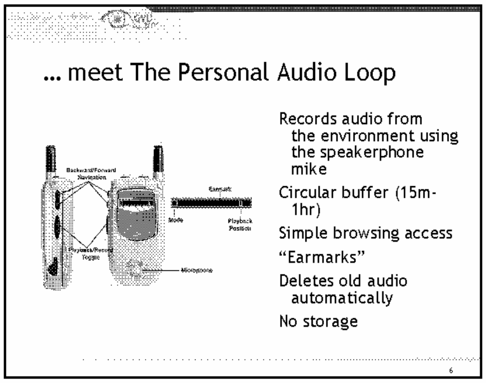
Security / Privacy Issues In Ubicomp

- Pervasive collection of information
  - from environments of everyday life
  - large amounts
- Invisibility of technology
- Continuous operation
- Lack of administration / supervision
- Legal issues



Did you ever experience this?

Your conversation is interrupted. When you resume, you can't remember what the topic was.



... meet The Personal Audio Loop

Backward/Forward Navigation
Earmark
Mode
Playback Position
Playback/Record Toggle
Microphone

Records audio from the environment using the speakerphone mike

Circular buffer (15m-1hr)

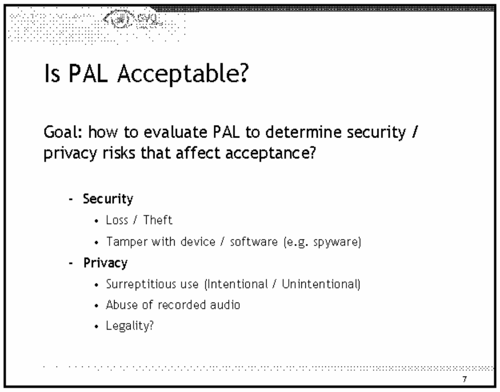
Simple browsing access

"Earmarks"

Deletes old audio automatically

No storage

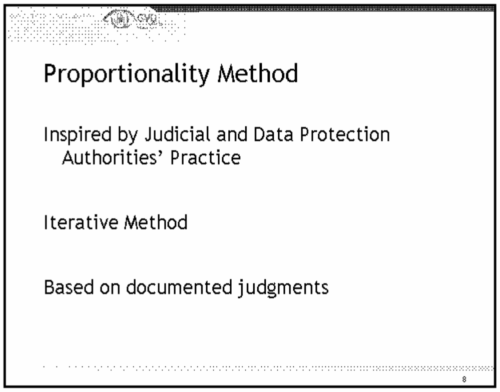
Figure B.8: Set of Lecture Slides Used In the Proportionality Condition.



Is PAL Acceptable?

Goal: how to evaluate PAL to determine security / privacy risks that affect acceptance?

- **Security**
  - Loss / Theft
  - Tamper with device / software (e.g. spyware)
- **Privacy**
  - Surreptitious use (Intentional / Unintentional)
  - Abuse of recorded audio
  - Legality?

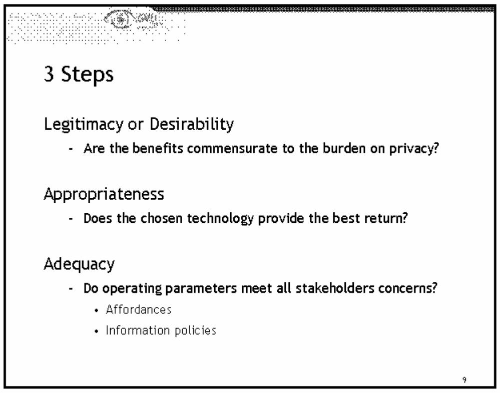


Proportionality Method

Inspired by Judicial and Data Protection Authorities' Practice

Iterative Method

Based on documented judgments



3 Steps

Legitimacy or Desirability

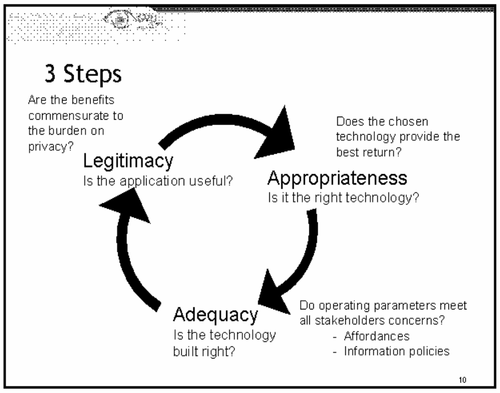
- **Are the benefits commensurate to the burden on privacy?**

Appropriateness

- **Does the chosen technology provide the best return?**

Adequacy

- **Do operating parameters meet all stakeholders concerns?**
  - Affordances
  - Information policies



3 Steps

Are the benefits commensurate to the burden on privacy?

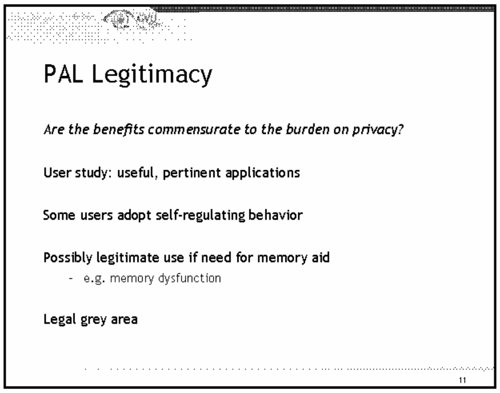
Legitimacy
Is the application useful?

Does the chosen technology provide the best return?

Appropriateness
Is it the right technology?

Do operating parameters meet all stakeholders concerns?
- Affordances
- Information policies

Adequacy
Is the technology built right?



PAL Legitimacy

Are the benefits commensurate to the burden on privacy?

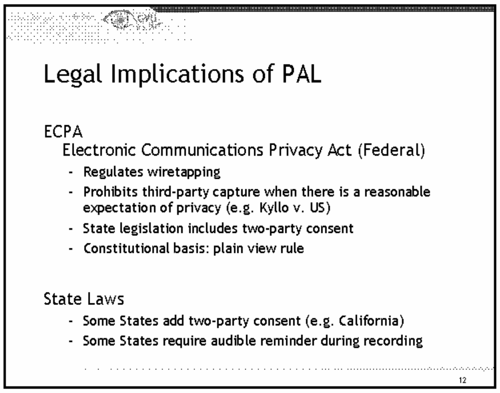
User study: useful, pertinent applications

Some users adopt self-regulating behavior

Possibly legitimate use if need for memory aid

- e.g. memory dysfunction

Legal grey area



Legal Implications of PAL

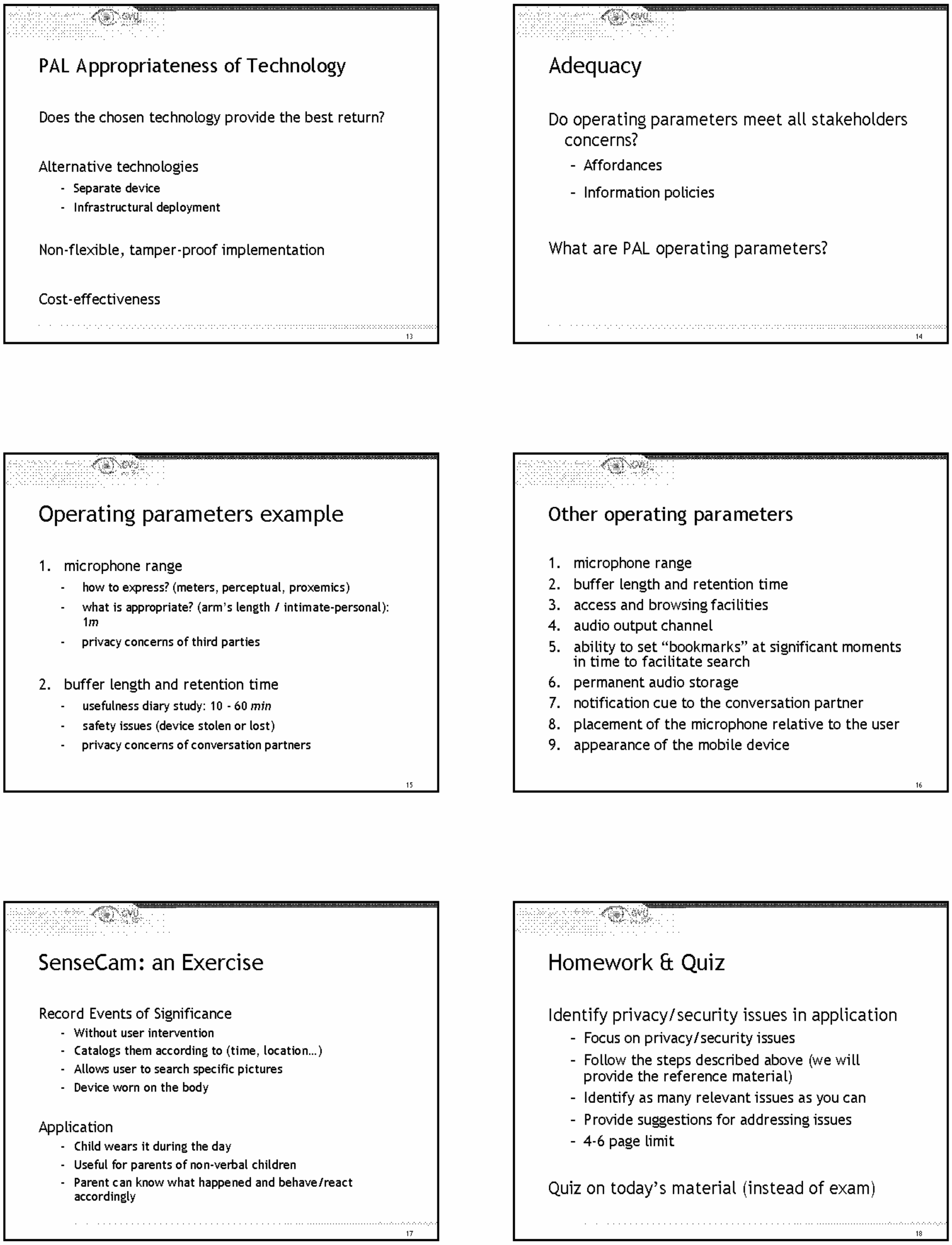
ECPA
Electronic Communications Privacy Act (Federal)

- **Regulates wiretapping**
- **Prohibits third-party capture when there is a reasonable expectation of privacy (e.g. Kyllo v. US)**
- **State legislation includes two-party consent**
- **Constitutional basis: plain view rule**

State Laws

- **Some States add two-party consent (e.g. California)**
- **Some States require audible reminder during recording**

Figure B.8: Set of Lecture Slides Used In the Proportionality Condition. (Continued.)



PAL Appropriateness of Technology

Does the chosen technology provide the best return?

Alternative technologies

- Separate device
- Infrastructural deployment

Non-flexible, tamper-proof implementation

Cost-effectiveness

13

Adequacy

Do operating parameters meet all stakeholders concerns?

- Affordances
- Information policies

What are PAL operating parameters?

14

Operating parameters example

1. microphone range
   - how to express? (meters, perceptual, proxemics)
   - what is appropriate? (arm's length / intimate-personal): 1*m*
   - privacy concerns of third parties
2. buffer length and retention time
   - usefulness diary study: 10 - 60 *min*
   - safety issues (device stolen or lost)
   - privacy concerns of conversation partners

15

Other operating parameters

1. microphone range
2. buffer length and retention time
3. access and browsing facilities
4. audio output channel
5. ability to set "bookmarks" at significant moments in time to facilitate search
6. permanent audio storage
7. notification cue to the conversation partner
8. placement of the microphone relative to the user
9. appearance of the mobile device

16

SenseCam: an Exercise

Record Events of Significance

- Without user intervention
- Catalogs them according to (time, location…)
- Allows user to search specific pictures
- Device worn on the body

Application

- Child wears it during the day
- Useful for parents of non-verbal children
- Parent can know what happened and behave/react accordingly

17

Homework & Quiz

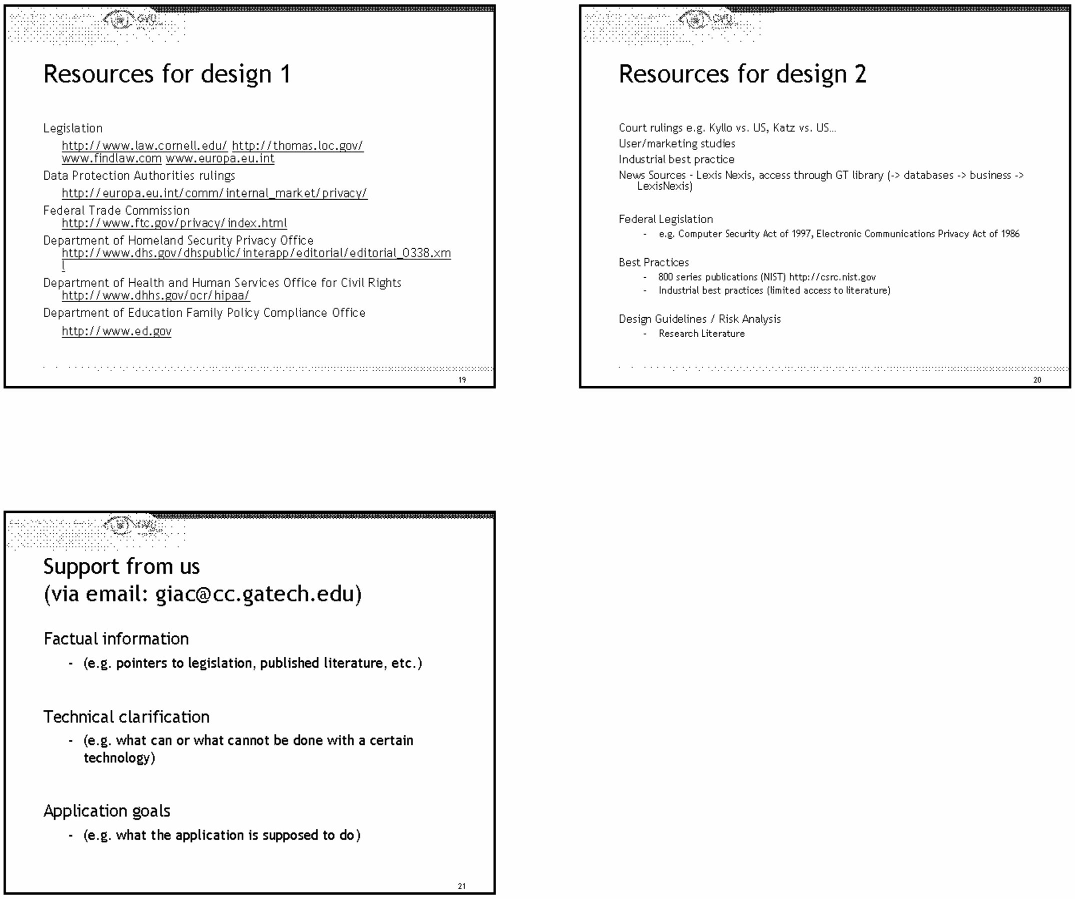
Identify privacy/security issues in application

- Focus on privacy/security issues
- Follow the steps described above (we will provide the reference material)
- Identify as many relevant issues as you can
- Provide suggestions for addressing issues
- 4-6 page limit

Quiz on today's material (instead of exam)

18

Figure B.8: Set of Lecture Slides Used In the Proportionality Condition. (Continued.)



Resources for design 1

Legislation

http://www.law.cornell.edu/ http://thomas.loc.gov/
www.findlaw.com www.europa.eu.int

Data Protection Authorities rulings

http://europa.eu.int/comm/internal_market/privacy/

Federal Trade Commission
http://www.ftc.gov/privacy/index.html

Department of Homeland Security Privacy Office
http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0338.xml

Department of Health and Human Services Office for Civil Rights
http://www.dhhs.gov/ocr/hipaa/

Department of Education Family Policy Compliance Office

http://www.ed.gov

19

Resources for design 2

Court rulings e.g. Kyllo vs. US, Katz vs. US...
User/marketing studies
Industrial best practice
News Sources - Lexis Nexis, access through GT library (-> databases -> business -> LexisNexis)

Federal Legislation
- e.g. Computer Security Act of 1997, Electronic Communications Privacy Act of 1986

Best Practices
- 800 series publications (NIST) http://csrc.nist.gov
- Industrial best practices (limited access to literature)

Design Guidelines / Risk Analysis
- Research Literature

20

Support from us
(via email: giac@cc.gatech.edu)

Factual information
- **(e.g. pointers to legislation, published literature, etc.)**

Technical clarification
- **(e.g. what can or what cannot be done with a certain technology)**

Application goals
- **(e.g. what the application is supposed to do)**

21

Figure B.8: Set of Lecture Slides Used In the Proportionality Condition. (Continued.)

B.4 Pilot Study Assignment

The text below reports one of the project descriptions used in the design method evaluation pilot study.

“CS6725 Security Strategy Course

Mobile Location-Enhanced Person Finder

Project Description

Location technologies are becoming increasingly commonplace on a variety of platforms, including cell phones and portable computers. One class of applications supported by these technologies consists in people finder tools. Usually implemented on cell phones, these tools allow a user to ask for the location of another person and reply to such requests. Early user testing suggest that people may find person finders very valuable. At least one such application has been marketed in the United States, by AT&T Wireless.

We desire to implement a person finder application that runs on a cell phone, which would allow users to ask the location and respond to location requests. These messages can then be used for a variety of reasons, including meeting up, either in person or per phone, assessing the availability of the other person, or as a status notification to coordinate joint activities.

The confidentiality of people’s location data used for call routing has been traditionally covered by specific legislation. However, the broader use of location information within social groups and organizations my raise concerns relating to its security, control and user privacy. The collected information is personally identifiable and may be used to track individuals, which could lead to stalking incidents, as well as commercial exploitation.

A variety of different architectures can be used for developing such applications, including server-based, device-based and mixed. Moreover, several alternative location sensing techniques can be employed.

Project Assignment

In this project you will be asked to design (not to implement) a person finder application, and specifically, you will be asked to define information management and/or organizational policies of the application and the aspects of the user interface that have security and privacy implications. You will be asked to justify your technical and organizational design choices. You will reference federal and state regulation, industry guidelines and other sources.

The resulting design should be technically and organizationally feasible, given existing available technology and considering the organizational structure of deployment.

You will be asked to follow a general design method, provided by us, for the analysis of security and privacy requirements. [G. Iachello & G. Abowd: "Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design In Ubiquitous Computing"]

Research Study

You will be asked to participate in a research study with the purpose of assessing the effectiveness and usefulness of the above mentioned design method. Your participation in this research study is voluntary. If you don't want to be in this study you have the option of choosing another project for completing your CS6725 requirements.

Milestones and deliverables

Mar 15 – Mid-project milestone

On this date you will turn in a written document, encompassing the initial analysis of the problem, which should include at least the following items:

- Project definition, including application goals.
- Short exploration of 2 – 4 Alternative designs. This will allow both to explore the design space and will inform the final design you choose. It is important to include here a concise description of each design, what makes it different from the others and what its peculiar characteristics in terms of security and privacy are.
- Identification of involved stakeholders and concerns. This should include a list of direct and indirect stakeholders in your system, and a discussion

of how these stakeholders relate and are affected by it. Also, you should include a discussion of the points of contact of your application/system with other organizational entities.

- Identification of design resources. This should include an initial exploration of existing sector literature, regulation, technical sources, and any other sources you may find useful for conducting your analysis.

Apr 14 – Final Deliverable

At the end of the project you will be expected to produce a final design document which should include at least the following:

- Regulatory constraints.
- Experience from similar applications.
- Description of system design.
- Discussion of the selected design for the system. Information management policies. Technical safeguards for securing data and people, including which aspects of the user interface of the system you consider relevant (e.g. how the system is operated, accessed, etc.) Indicate how you address all stakeholder concerns within your design.
- Organizational measures to be adopted with system use. It is important that you justify in some way all the major or potentially divisive choices you make in your design. Take advantage of all available sources for gathering supporting arguments for your choices.

You will be asked to present in class your project. You will be given a time slot still to be defined between 10 and 30 minutes, including question time.

Your project will be graded both on the quality of your written submission and of that of your presentation.

Initial Sources List

The following is an initial list of sources for your project. It is not meant to be exhaustive! You are strongly encouraged to consult other sources as you may find appropriate.

- US Federal Communications Commission (www.fcc.gov) guidelines and policy.
- Similar existing applications. (E.g. AT&T Find People Nearby)

- Existing US Regulation. If your design is meant to work in other jurisdictions, include and discuss the impact of one example of regulation from that country(ies).
- Journals in the telecommunication sector (e.g. Education Resource Information Center, PsychArticles, both are searchable on the EBSCO database accessible through the Georgia Tech Library)
- News sources such as Lexis Nexis (available through the Georgia Tech Library)

Further support

If you want to ask me (Giovanni) specific questions, I will be available after class on Tuesdays or by appointment (email me to schedule)."

APPENDIX C

EVALUATION STUDY STATISTICAL DATA

C.1 Means Comparison Across Conditions

Tables C.1 and C.2 show the descriptive statistics and the mean differences significance of select metrics in the design method evaluation study.

Table C.1: Descriptive Statistics of Relevant Metrics.

Condition		**Feedback / Control**	**Risk Analysis**	**Proportionality**	**Design Rationale**	**Total**
T Number of Identified Security/Privacy Issues	N	11	12	13	12	48
	Mean	5.18**	7.83**	6.85	6.25	6.56
	Std. Dev.	3.31	3.24	2.34	1.66	2.78
	Min	2	3	3	4	2
	Max	13	12	11	9	13
C Number of Design Choices	N	11	12	13	12	48
	Mean	10.64	9.33	10.08	8.42	9.60
	Std. Dev.	3.88	2.67	3.99	5.26	4.01
	Min	4	6	2	3	2
	Max	16	14	15	22	22
N Number of Scenarios	N	11	12	13	12	48
	Mean	0.18	0.00	0.08	0.00	0.06
	Std. Dev.	0.40	0.00	0.28	0.00	0.24
	Min	0	0	0	0	0
	Max	1	0	1	0	1
X Number of Comparisons with Similar Applications	N	11	12	13	12	48
	Mean	0.00	0.00	0.62	0.33	0.25
	Std. Dev.	0.00	0.00	0.77	0.89	0.64
	Min	0	0	0	0	0
	Max	0	0	2	3	3
S Number of Stakeholders	N	11	12	13	12	48
	Mean	6.82	4.75	5.23	6.42	5.77
	Std. Dev.	3.09	1.60	1.17	2.84	2.36
	Min	1	3	4	3	1
	Max	11	9	8	13	13

** Difference in means significant $p < 0.05$.

Table C.1: Descriptive Statistics of Relevant Metrics. (Continued.)

Condition		**Feedback / Control**	**Risk Analysis**	**Proportionality**	**Design Rationale**	**Total**
O Number of Openended Issues	N	11	12	13	12	48
	Mean	0.36**	0.25**	1.69**	0.83	0.81
	Std. Dev.	0.50	0.62	1.25	1.59	1.21
	Min	0	0	0	0	0
	Max	1	2	4	5	5
V Number of Value Propositions	N	11	12	13	12	48
	Mean	1.36	2.00**	1.92	0.75**	1.52
	Std. Dev.	0.81	1.28	1.55	0.62	1.22
	Min	0	1	0	0	0
	Max	3	5	6	2	6
Z Size of the Deliverable	N	11	12	13	12	48
	Mean	24.55	24.17	26.46	23.00	24.58
	Std. Dev.	7.19	4.86	7.13	7.07	6.55
	Min	14	16	11	13	11
	Max	35	33	37	36	37
G Grade (1–10)	N	11	12	13	12	48
	Mean	8.77	8.21	8.65	8.46	8.52
	Std. Dev.	1.54	1.03	0.69	0.72	1.02
	Min	5	6	8	7	5
	Max	10	10	10	10	10
Q Quality (0–6)	N	11	12	13	12	48
	Mean	4.24**	3.21**	3.96	3.83	3.81
	Std. Dev.	0.99	0.79	0.95	0.93	0.96
	Min	2.2	2.2	1.8	2.5	1.8
	Max	5.5	4.2	5.2	5.3	5.5

Table C.1: Descriptive Statistics of Relevant Metrics. (Continued.)

Condition		**Feedback / Control**	**Risk Analysis**	**Proportionality**	**Design Rationale**	**Total**
A Adherence (0.0–1.0)	N	11	12	13	12	48
	Mean	0.80	0.66	0.71	0.93	0.78
	Std. Dev.	0.37	0.30	0.21	0.13	0.28
	Min	0.00	0.00	0.27	0.60	0.00
	Max	1.00	1.00	1.00	1.00	1.00

Table C.2: Tukey HSD Means Comparison.

Dependent Variable	**(I) Condition**	**(J) Condition**	**Mean Difference (I-J)**	**Std. Error**	**Sig.**	**95% Confidence Interval**	
						Lower Bound	**Upper Bound**
Number of Identified Security/Privacy Issues	1	2	-3.43(*)	1.041	.010	-6.21	-.65
		3	-2.45	1.022	.094	-5.18	.29
		4	-1.85	1.041	.298	-4.63	.93
	2	1	3.43(*)	1.041	.010	.65	6.21
		3	.99	.973	.742	-1.61	3.59
		4	1.58	.992	.392	-1.07	4.24
	3	1	2.45	1.022	.094	-.29	5.18
		2	-.99	.973	.742	-3.59	1.61
		4	.60	.973	.927	-2.00	3.20
	4	1	1.85	1.041	.298	-.93	4.63
		2	-1.58	.992	.392	-4.24	1.07
		3	-.60	.973	.927	-3.20	2.00
Number of Scenarios	1	2	.18	.101	.284	-.09	.45
		3	.10	.099	.714	-.16	.37
		4	.18	.101	.284	-.09	.45
	2	1	-.18	.101	.284	-.45	.09
		3	-.08	.097	.856	-.33	.18
		4	.00	.098	1.000	-.26	.26
	3	1	-.10	.099	.714	-.37	.16
		2	.08	.097	.856	-.18	.33
		4	.08	.097	.856	-.18	.33
	4	1	-.18	.101	.284	-.45	.09
		2	.00	.098	1.000	-.26	.26
		3	-.08	.097	.856	-.33	.18

* The mean difference is significant at the .05 level.

Table C.2: Tukey HSD Means Comparison. (Continued.)

Dependent Variable	(I) Condition	(J) Condition	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Number of Comparisons with Similar Applications	1	2	.00	.250	1.000	-.67	.67
		3	-.62	.245	.072	-1.27	.04
		4	-.33	.250	.546	-1.00	.33
	2	1	.00	.250	1.000	-.67	.67
		3	-.62	.239	.063	-1.25	.02
		4	-.33	.244	.528	-.99	.32
	3	1	.62	.245	.072	-.04	1.27
		2	.62	.239	.063	-.02	1.25
		4	.28	.239	.644	-.36	.92
	4	1	.33	.250	.546	-.33	1.00
		2	.33	.244	.528	-.32	.99
		3	-.28	.239	.644	-.92	.36
Number of Stakeholders	1	2	2.07	.953	.147	-.48	4.61
		3	1.59	.935	.337	-.91	4.08
		4	.40	.953	.975	-2.14	2.94
	2	1	-2.07	.953	.147	-4.61	.48
		3	-.48	.913	.952	-2.92	1.96
		4	-1.67	.932	.292	-4.15	.82
	3	1	-1.59	.935	.337	-4.08	.91
		2	.48	.913	.952	-1.96	2.92
		4	-1.19	.913	.569	-3.62	1.25
	4	1	-.40	.953	.975	-2.94	2.14
		2	1.67	.932	.292	-.82	4.15
		3	1.19	.913	.569	-1.25	3.62

Table C.2: Tukey HSD Means Comparison. (Continued.)

Dependent Variable	(I) Condition	(J) Condition	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Number of Design Choices	1	2	1.30	1.694	.868	-3.22	5.83
		3	.56	1.663	.987	-3.88	5.00
		4	2.22	1.694	.562	-2.30	6.74
	2	1	-1.30	1.694	.868	-5.83	3.22
		3	-.74	1.625	.968	-5.08	3.60
		4	.92	1.657	.945	-3.51	5.34
	3	1	-.56	1.663	.987	-5.00	3.88
		2	.74	1.625	.968	-3.60	5.08
		4	1.66	1.625	.738	-2.68	6.00
	4	1	-2.22	1.694	.562	-6.74	2.30
		2	-.92	1.657	.945	-5.34	3.51
		3	-1.66	1.625	.738	-6.00	2.68
Number of Openended Issues	1	2	.11	.459	.995	-1.11	1.34
		3	-1.33(*)	.451	.025	-2.53	-.13
		4	-.47	.459	.737	-1.70	.76
	2	1	-.11	.459	.995	-1.34	1.11
		3	-1.44(*)	.440	.011	-2.62	-.27
		4	-.58	.449	.568	-1.78	.62
	3	1	1.33(*)	.451	.025	.13	2.53
		2	1.44(*)	.440	.011	.27	2.62
		4	.86	.440	.222	-.32	2.03
	4	1	.47	.459	.737	-.76	1.70
		2	.58	.449	.568	-.62	1.78
		3	-.86	.440	.222	-2.03	.32

Table C.2: Tukey HSD Means Comparison. (Continued.)

Dependent Variable	**(I) Condition**	**(J) Condition**	**Mean Difference (I-J)**	**Std. Error**	**Sig.**	**95% Confidence Interval**	
						Lower Bound	**Upper Bound**
Number of Value Propositions	1	2	-.64	.478	.549	-1.91	.64
		3	-.56	.469	.635	-1.81	.69
		4	.61	.478	.578	-.66	1.89
	2	1	.64	.478	.549	-.64	1.91
		3	.08	.458	.998	-1.15	1.30
		4	1.25(*)	.468	.050	.00	2.50
	3	1	.56	.469	.635	-.69	1.81
		2	-.08	.458	.998	-1.30	1.15
		4	1.17	.458	.065	-.05	2.40
	4	1	-.61	.478	.578	-1.89	.66
		2	-1.25(*)	.468	.050	-2.50	.00
		3	-1.17	.458	.065	-2.40	.05
Size of the Deliverable	1	2	.38	2.769	.999	-7.01	7.77
		3	-1.92	2.717	.895	-9.17	5.34
		4	1.55	2.769	.944	-5.85	8.94
	2	1	-.38	2.769	.999	-7.77	7.01
		3	-2.29	2.655	.823	-9.38	4.79
		4	1.17	2.708	.973	-6.06	8.40
	3	1	1.92	2.717	.895	-5.34	9.17
		2	2.29	2.655	.823	-4.79	9.38
		4	3.46	2.655	.566	-3.63	10.55
	4	1	-1.55	2.769	.944	-8.94	5.85
		2	-1.17	2.708	.973	-8.40	6.06
		3	-3.46	2.655	.566	-10.55	3.63

Table C.2: Tukey HSD Means Comparison. (Continued.)

Dependent Variable	**(I) Condition**	**(J) Condition**	**Mean Difference (I-J)**	**Std. Error**	**Sig.**	**95% Confidence Interval**	
						Lower Bound	**Upper Bound**
Grade	1	2	.56	.431	.561	-.59	1.71
		3	.12	.423	.992	-1.01	1.25
		4	.31	.431	.885	-.84	1.46
	2	1	-.56	.431	.561	-1.71	.59
		3	-.45	.413	.704	-1.55	.66
		4	-.25	.421	.933	-1.37	.87
	3	1	-.12	.423	.992	-1.25	1.01
		2	.45	.413	.704	-.66	1.55
		4	.20	.413	.965	-.91	1.30
	4	1	-.31	.431	.885	-1.46	.84
		2	.25	.421	.933	-.87	1.37
		3	-.20	.413	.965	-1.30	.91
Quality	1	2	1.034(*)	.3812	.045	.016	2.052
		3	.281	.3742	.876	-.718	1.280
		4	.409	.3812	.708	-.609	1.427
	2	1	-1.034(*)	.3812	.045	-2.052	-.016
		3	-.753	.3656	.182	-1.729	.223
		4	-.625	.3729	.348	-1.621	.371
	3	1	-.281	.3742	.876	-1.280	.718
		2	.753	.3656	.182	-.223	1.729
		4	.128	.3656	.985	-.848	1.104
	4	1	-.409	.3812	.708	-1.427	.609
		2	.625	.3729	.348	-.371	1.621
		3	-.128	.3656	.985	-1.104	.848

REFERENCES

[1] 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 *Official Journal of the European Communities*, L281 (1995) 31–50.

[2] Directive 1999/93/EC Of The European Parliament And Of The Council of 13 December 1999 on a Community framework for electronic signatures *Official Journal of the European Communities*, L13 (1999) 12–20.

[3] 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) *Official Journal of the European Communities*, L201 (2002) 37-47.

[4] *Dodgeball web site*. (2004). Available from: http://www.dodgeball.com/

[5] Katz v. United States, S.Ct.; 389 U.S. 347; 88 S.Ct. 507 (1967).

[6] Kyllo v. United States, S.Ct.; 533 U.S. 27 (2001).

[7] United Kingdom Data Protection Act (1998).

[8] United States Electronic Communications Privacy Act of 1986, *18 USC 2510 et seq.* (1986).

[9] United States Family Educational and Privacy Rights Act, *20 USC 1232g et seq.* (1974).

[10] United States Health Insurance Portability And Accountability Act, *42 USC 1179* (1999).

[11] United States Sarbanes-Oxley Act, P.L. 107-204 (2002).

[12] United States Video Voyeurism Prevention Act, *18 USC 1801 et seq.* (2004).

[13] Volkszählungsurteil vom 15. Dezember 1983, BVerfGE 65,1, German Constitutional Court (Bundesverfassungsgerichts) (1983).

[14] Abowd, G.D. and Mynatt, E.D. Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 7, 1 (2000) 29–58.

[15] Ackerman, M.S., Cranor, L. and Reagle, J. Privacy in e-commerce: examining user scenarios and privacy preferences. *Proc. ACM conference on electronic commerce (EC'99)*. Denver, Colorado (1999) 1–8.

[16] Acquisti, A. and Grossklags, J. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*, 3, 1 (2005) 26–33.

[17] Adams, A. and Blandford, A. Bridging the gap between organizational and user perspectives of security in the clinical domain. *Int. J. Human-Computer Studies*, 63 (2005) 175–202.

[18] Adams, A. and Sasse, M.A. Privacy in Multimedia Communications: Protecting Users, Not Just Data. *Proc. Human-Computer Interaction/Interaction d'Homme-Machine (IMH-HCI 01)*. Lille, France: Springer Verlag (2001) 49–64.

[19] Alexander, C. *The Timeless Way Of Building*, Oxford University Press: New York, NY, USA (1979) ISBN: 0-19-502402-8.

[20] Altman, I. *The Environment and Social Behavior—Privacy, Personal Space, Territory, Crowding*, Brooks/Cole Publishing Company: Monterey, CA (1975) ISBN: 0-8185-0168-5.

[21] Altman, I. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33, 3 (1977) 66–84.

[22] Arnold, M. On the phenomenology of technology: the "Janus-faces" of mobile phones. *Information and Organization*, 13 (2003) 231–256.

[23] Association for Computing Machinery. *ACM Code of Ethics*. Available from: http://www.acm.org/serving/ethics.html. Last accessed: 3/21/2006.

[24] AT&T Wireless. *Find People Nearby*. Available from: http://www.attwireless.com/personal/features/organization/findfriends.jhtml. Last accessed: 3/1/2003.

[25] Barkhuus, L. and Dey, A. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. *Proc. Interact 2003*. Zurich, Switzerland: ACM Press (2003) 709–712.

[26] Barofsky, A. The European Commisssion's Directive On Electronic Signatures: Technological "Favoritism" Towards Digital Signatures. *Boston College International & Comparative Law Review*, 24, 1 (2000) 145–160.

[27] Barrett, R., Kandogan, E., Maglio, P.P., Haber, E.M., Takayama, L.A. and Prabaker, M. Field Studies of Computer System Administrators: Analysis of System Management Tools and Practices. *Proc. CSCW '04*, 6(3). Chicago, IL, USA: ACM Press (2004) 388–395.

[28] Bäumler, H., Federrath, H. and Golembiewski, C., *Report on the Criminal Justice Process against "AN.ON - Anonymity.Online"*, TU-Dresden, Germany (2003). Available from: http://anon.inf.tu-dresden.de/strafverfolgung/index_en.html. Last accessed: 2/17/2006.

[29] Beckwith, R. and Lederer, S. Designing One's Dotage: Ubicomp in Residential Care Facilities. *Proc. Home-Oriented Informatics and Telematics HOIT 03*: Center for Research on Information Technology and Organizations (2003).

[30] Belair, R. and Bock, C., *Police Use of Remote Camera Systems for Surveillance of Public Streets*, in *Surveillance, Dataveillance and Personal Freedoms: Use and Abuse of Information Technology*. Burdick: Fair Lawn, NJ, USA (1973).

[31] Bellotti, V. and Sellen, A. Design for Privacy in Ubiquitous Computing Environments. *Proc. ECSCW '93*: Kluwer A.P., Dordrecht, The Netherlands (1993) 77–92.

[32] Bennet, C. and Grant, R., Editors, *Visions of Privacy: Policy Choices for the Digital Age*, University of Toronto: Toronto, Canada (1999) ISBN: 0-8020-8050-2.

[33] Berendt, B., Günther, O. and Spiekermann, S. Privacy in e-commerce: stated preferences vs. actual behavior *Communications of the ACM*, 48, 4 (2005) 101–106.

[34] Beresford, A.R. and Stajano, F. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2, 1 (2003) 46–55.

[35] Berleur, J. and Brunnstein, K., Editors, *Ethics of Computing: Codes, spaces for discussion and law*, Chapman & Hall: London, England (1996) ISBN: 0-412-72620-3.

[36] Boehm, B.W., Bose, P., Horowitz, E. and Lee, M.J. Software Requirements As Negotiated Win Conditions. *Proc. First International Conference on Requirements Engineering*: IEEE Press (1994) 74–83.

[37] Böhm, A., Leiber, T. and Reufenheuser, B. Trust and Transparency in Location-Based Services: Making Users lose their Fear of Big Brother. *Proc. Mobile HCI 2004 Workshop On Location Systems Privacy and Control*. Glasgow, UK (2004).

[38] Boyle, M., Edwards, C. and Greenberg, S. The effects of filtered video on awareness and privacy. *Proc. ACM CSCW 2000*: ACM Press (2000) 1–10.

[39] Boyle, M. and Greenberg, S. The language of privacy: Learning from video media space analysis and design *ACM Transactions on Computer-Human Interaction (TOCHI)*, 12, 2 (2005).

[40] British Institute of International and Comparative Law, *The implementation of Directive 95/46/EC to the Processing of Sound and Image Data* (2003). Available from: http://www.europa.eu.int

[41] Buchenau, M. and Suri, J.F. Experience Prototyping. *Proc. DIS 2000*: ACM Press (2000) 424–433.

[42] Chalmers, M. A Historical View of Context. *Computer Supported Cooperative Work*, 13, 3–4 (2004) 223–247.

[43] Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24, 2 (1981) 84–88.

[44] Christensen, C.M., Anthony, S.D. and Roth, E.A. *Seeing What's Next: Using Theories of Innovation to Predict Industry Change*, Harvard Business School Press: Boston, MA, USA (2004) ISBN: 1591391857.

[45] Chung, E., Jason, H., Lin, J., Prabaker, M., Landay, J. and Liu, A. Development and Evaluation of Emerging Design Patterns for Ubiquitous Computing. *Proc. DIS 2004*: ACM Press (2004) 233–242.

[46] Chung, E., Jason, H., Lin, J., Prabaker, M., Landay, J. and Liu, A. *Ubicomp Design Patterns*. (2004). Available from: http://guir.berkeley.edu/projects/patterns/. Last accessed: 3/22/2006.

[47] Clarke, R. Person-Location and Person-Tracking: Technologies, Risks and Policy Implications. *Information Technology & People*, 14, 2 (2001) 206–231.

[48] Columbia Human Rights Law Review, Editor *Surveillance, Dataveillance and Personal Freedoms: Use and Abuse of Information Technology,* Burdick: Fair Lawn, NJ, USA (1973) ISBN: 0-913638-03-X.

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

[50] Commission of the European Communities, *Information Technology Security Evaluation Criteria, Version 1.2,* Technical Report, Commission of the European Communities, Brussels (1991).

[51] Consolvo, S., Smith, I., Matthews, T., LaMarca, A., Tabert, J. and Powledge, P. Location Disclosure to Social Relations: Why, When, & What People Want to Share. *Proc. CHI 2005*: ACM Press (2005) 82–90.

[52] Covington, M.J. A Context-Aware Security Architecture for Emerging Applications. *Proc. ACSAC '02*: IEEE Press (2002) 249–258.

[53] Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, Standard DoD 5200.28-STD, Department of Defense (1985).

[54] DePaulo, B.M. and Kashy, D.A. Everyday Lies in Close and Casual Relationships. *Journal of Personality and Social Psychology*, 74, 1 (1998) 63–79.

[55] Dey, A.K., Salber, D. and Abowd, G.D. A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications. *Human-Computer Interaction (HCI) Journal*, 16, 2–4 (2001) 97–166.

[56] Dix, A., Finlay, J., Abowd, G. and Beale, R. *Human Computer Interaction (2nd ed.)*, Prentice Hall Europe: London (1998).

[57] Dourish, P. What We Talk About When We Talk About Context. *Personal and Ubiquitous Computing*, 8, 1 (2004) 19–30.

[58] Dow, S., Lee, J., Oezbek, C., MacIntyre, B., Bolter, J.D. and Gandy, M. Exploring Spatial Narratives and Mixed Reality Experiences in Oakland Cemetery. *Proc. Advances in Computer Entertainment ACE'05*: ACM Press (2005).

[59] Duckham, M. and Kulik, L. A Formal Model of Obfuscation and Negotiation for Location Privacy. *Proc. Pervasive 2005*, LNCS 3468. Munich, Germany: Springer Verlag (2005) 152–170.

[60] Etzioni, A. *The Limits of Privacy*, Basic Books: New York, NY, USA (1999) ISBN: 0-465-04090-X.

[61] European Commission Article 29 Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, 11750/02/EN WP 89 (2004). Available from: http://www.europa.eu.int

[62] European Commission Article 29 Working Party, *Working Document on Biometrics*, 12168/02/EN WP80 (2004). Available from: http://europa.eu.int

[63] Fallman, D. Design-oriented Human-Computer Interaction. *Proc. CHI 2003*. Ft. Lauderdale, Florida, USA: ACM Press (2003) 225–232.

[64] Federal Communications Commission, *Third Report And Order And Third Further Notice Of Proposed Rulemaking*, FCC-02-214A1 (2002). Available from: http://www.fcc.gov

[65] Federal Trade Commission, *National and State Trends in Fraud & Identity Theft January - December 2004*, Federal Trade Commission (2005). Available from: http://www.consumer.gov/idtheft/pdf/clearinghouse_2004.pdf. Last accessed: 3/21/2006.

[66] Federal Trade Commission, Standards for Safeguarding Customer Information; Final Rule, *16 CFR Part 314*.

[67] Fogg, B.J., Soohoo, C., Danielson, D.R., Marable, L., Stanford, J. and Tauber, E.R. How do users evaluate the credibility of Web sites?: a study with over 2,500 participants. *Proc. Designing for User Experiences*: ACM Press (2003) 1–15

[68] Friedman, B. Value-Sensitive Design. *Interactions: New Visions of Human-Computer Interaction*, 3, 6 (1996) 17–23.

[69] Garfinkel, S. Adopting Fair Information Practices to Low Cost RFID Systems. *Proc. Ubiquitous Computing 2002 Privacy Workshop* (2002).

[70] Garfinkel, S. and Rosenberg, B., Editors, *RFID : Applications, Security, and Privacy*, Addison-Wesley Professional (2005) ISBN: 0321290968.

[71] Gates, W. *Trustworthy Computing*. (2002). Available from: http://www.wired.com/news/business/0,1367,49826,00.html. Last accessed: 3/21/2006.

[72] Gaver, W., Moran, T., MacLean, A., Lovstrand, L., Dourish, P., Carter, K. and Buxton, W. Realizing a Video Environment: EuroPARC's RAVE System. *Proc. CHI'92*. Monterey, CA, USA: ACM Press (1992) 27–35.

[73] Geason, S. and Wilson, P. *Preventing graffiti and vandalism*, Australian Institute of Criminology: Canberra, Australia (1990) ISBN: 0-642-14936-4.

[74] Gedik, B. and Liu, L., *A Customizable k-Anonymity Model for Protecting Location Privacy*, GIT-CERCS-04-15, Georgia Institute of Technology, Atlanta, GA, USA (2004). Available from: http://www.cercs.gatech.edu/tech-reports/tr2004/git-cercs-04-15.pdf. Last accessed: 3/21/2006.

[75] Gemmell, J., Williams, L., Wood, K., Lueder, R. and Bell, G. Passive Capture and Ensuing Issues for a Personal Lifetime Store. *Proc. CARPE'04*: ACM Press (2004) 48–55.

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

[77] Goffman, E. *Behavior In Public Places*, Free Press (1966) ISBN: 0029119405.

[78] Goffman, E. *The Presentation of Self in Everyday Life,* Anchor Books (1959) ISBN: 0385094027.

[79] Goldschlag, D.M., Reed, M.G. and Syverson, P.F. Hiding Routing Information. *Proc. Information Hiding*, LNCS 1174: Springer-Verlag (1996) 137–150.

[80] Grinter, R., Dourish, P., Delgado de la Flor, J. and Joseph, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004) 391–401.

[81] Gruteser, M. and Grunwald, D. Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: A Quantitative Analysis. *Proc. ACM International Workshop on Wireless Mobile Applications and Services on WLAN*: ACM Press (2003) 46–55.

[82] Günther, O. and Spiekermann, S. RFID And The Perception Of Control: The Consumer's View. *Communications of the ACM*, 48, 9 (2005) 73–76.

[83] GVU Center, *10th WWW User Survey – Online Privacy and Security*, GVU Center, Georgia Insitute of Technology (1999). Available from: http://www.gvu.gatech.edu/user_surveys/survey-1998-10/graphs/graphs.html#privacy. Last accessed: 3/21/2006.

[84] Hall, E. *The Hidden Dimension: Man's use of Space in Public and Private*, Doubleday: New York, NY, USA (1966).

[85] Hancock, J.T., Thom-Santelli, J. and Ritchie, T. Deception and Design: The Impact of Communication Technology on Lying Behavior. *Proc. CHI 2004*. Vienna, Austria: ACM Press (2004) 129–134.

[86] Hayes, G.R., Kientz, J., Truong, K.N., White, D., Abowd, G.D. and Pering, T. Designing Capture Applications to Support the Education of Children with Autism. *Proc. Ubicomp 2004*, LNCS 3205: Springer Verlag (2004) 161–178.

[87] Hayes, G.R., Patel, S.N., Truong, K.N., Iachello, G., Kientz, J.A., Farmer, R. and Abowd, G.D. The Personal Audio Loop: Designing a Ubiquitous Audio-Based Memory Aid. *Proc. Mobile HCI 2004*, LNCS 3160. Glasgow, Scotland: Springer Verlag (2004) 168–179.

[88] Hayes, G.R., Truong, K.N., Abowd, G.D. and Pering, T. Experience buffers: a socially appropriate, selective archiving tool for evidence-based care. *Proc. CHI 2005*. Portland, OR, USA: ACM Press (2005) 1435–1438.

[89] Helmers, S. *A Brief History of anon.penet.fi — The Legendary Anonymous Remailer* Computer-Mediated Communication Magazine (1997). Available from: http://www.december.com/cmc/mag/1997/sep/helmers.html. Last accessed: 2/10/2006.

[90] Hilty, L.M., Som, C. and Köhler, A. Assessing the Human, Social and Environmental Risks of Pervasive Computing. *Human and Ecological Risk Assessment*, 10 (2004) 853–874.

[91] Hong, J. and Landay, J. An Architecture for Privacy-Sensitive Ubiquitous Computing. *Proc. MobiSys '04*. Boston, MA, USA: ACM Press (2004) 177–189.

[92] Hong, J., Ng, J.D., Lederer, S. and Landay, J.A. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. *Proc. DIS 2004*: ACM Press (2004) 91–100.

[93] Hudson, S. and Smith, I. Techniques for Addressing Fundamental Privacy and Disruption Tradeoffs in Awareness Support Systems. *Proc. CSCW ’96*: ACM Press (1996) 248–257.

[94] Humphrey, W.S. *PSP: A Self-Improvement Process for Engineers*, Addison-Wesley (2005) ISBN: 03213054931.

[95] Iachello, G., *Reno: from ‘privacy test bed’ to ‘communication tool’, Version 0.5*, Unpublished document, Intel Research Seattle (2005).

[96] Iachello, G. and Abowd, G.D., *Emerging Ubiquitous Computing Technologies and Security Management*, in *Information Security Policies and Practices*, Baskerville, R., Goodman, S. and Straub, D., Editors (in preparation).

[97] Iachello, G. and Abowd, G.D. Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design In Ubiquitous Computing. *Proc. Conference on Human Factors in Computer Systems*. Portland, OR, USA: ACM Press (2005) 91–100.

[98] Iachello, G. and Abowd, G.D., *A Token-based Access Control Mechanism for Automated Capture and Access Systems in Ubiquitous Computing*, GIT Technical Report GIT-GVU-05-06, Georgia Institute of Technology, GVU Center (2005). Available from: http://www.cc.gatech.edu/gvu/research/techreports.html

[99] Iachello, G., Smith, I., Consolvo, S., Abowd, G.D., Hughes, J., Howard, J., Potter, F., Scott, J., Sohn, T., Hightower, J. and LaMarca, A. Control, Deception, and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service. *Proc. Lecture Notes in Computer Science*, LNCS 3660: Springer Verlag (2005) 213–231.

[100] Iachello, G., Smith, I., Consolvo, S., Chen, M. and Abowd, G.D. Developing Privacy Guidelines for Social Location Disclosure Applications and Services. *Proc. Symposium On Usable Privacy and Security (SOUPS)*. Pittsburgh, PA, USA: ACM Press (2005) 65–76.

[101] Iachello, G., Truong, K.N., Abowd, G.D., Hayes, G.R. and Stevens, M. Event-Contingent Experience Sampling to Evaluate Ubicomp Privacy in the Real World. *Proc. Accepted to CHI 2006* (2006).

[102] Information Systems Security Association, *Generally Accepted Information Security Practices (GAISP)* (2004). Available from: http://www.issa.org/gaisp/gaisp.html

[103] International Labor Organization *Part II: Monitoring and Surveillance in the Workplace Conditions of Work*, ISBN: ISBN 92-2-108740-9.

[104] International Organization for Standardization / International Electrotechnical Commission, *ISO/IEC 17799:2000 Information technology — Code of practice for information security management* (2000).

[105] ISO/IEC, *IS15408: Common Criteria for Information Technology Security Evaluation* (2000).

[106] Jehl, D., *Domestic Surveillance: Congressional Leaders; Among Those Told of Program, Few Objected* New York Times, December 23, 2005.

[107] Jensen, C., *Designing For Privacy in Interactive Systems*, Doctoral Dissertation, Georgia Institute of Technology, Atlanta, GA, USA (2005).

[108] Jensen, C., Tullio, J., Potts, C. and Mynatt, E.D., *STRAP: A Structured Analysis Framework for Privacy*, GVU Technical Report 05-02, GVU Center, Georgia In-

stitute of Technology, Atlanta, GA, USA (2005). Available from: http://www.cc.gatech.edu/gvu/research/tr05_02.html. Last accessed: 2/10/2006.

[109] Jensen, L., Jensen, J., Feldman, S. and Cauffman, E. The Right to Do Wrong: Lying to Parents Among Adolescents and Emerging Adults. *Journal of Youth and Adolescence*, 33, 2 (2004) 101–112.

[110] Jiang, X., Hong, J.I. and Landay, J.A. Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing. *Proc. Ubicomp 2002*, LNCS 2498: Springer Verlag (2002) 176–193.

[111] Kindberg, T., Sellen, A. and Geelhoed, E. Security and Trust in Mobile Interactions: a Study of Users' Perceptions and Reasoning. *Proc. Ubicomp 2004*, LNCS 3205. Nottingham, UK: Springer Verlag (2004) 196–213.

[112] Kjeldskov, J. and Graham, C. A Review of Mobile HCI Research Methods. *Proc. Mobile HCI*, LNCS 2975: Springer Verlag (2003) 317–335.

[113] Knox, D., Zusman, M.E., McGinty, K. and Gescheidler, J. Deception of Parents During Adolescence. *Adolescence*, 36, 143 (2001).

[114] Konrad, R., *Calls for federal regulation grow as data retailer scandal widens*, The Associated Press State & Local Wire, 2/18/2005.

[115] Laasonen, K., Raento, M. and Toivonen, H. Adaptive On-Device Location Recognition. *Proc. Pervasive 2004*, LNCS 3001. Vienna, Austria: Springer Verlag (2004) 287–304.

[116] Langheinrich, M. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. *Proc. Ubicomp 2001*, LNCS 2201: Springer Verlag (2001) 273–291.

[117] Larson, R. and Csikszentmihalyi, M. The experience sampling method. *New Directions for Methodology of Social and Behavioral Science*, 15 (1983) 41–56.

[118] Latour, B. *We've never been modern*, Harvard University Press: Cambridge, MA, USA (1991) ISBN: 0-674-94839-4.

[119] Lederer, S., *Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing*, UC Berkeley Computer Science Division (2003).

[120] Lederer, S., Hong, J., Dey, A. and Landay, J., *Personal Privacy through Understanding and Action: Five Pitfalls for Designers*, IRB-TR-03-035, Intel (2003).

[121] Lessig, L. The Architecture of Privacy. *Vanderbilt Journal of Entertainment Law & Practice*, 1 (1999) 56.

[122] Li, Y., Hong, J. and Landay, J. Topiary: A Tool for Prototyping Location-Enhanced Applications. *Proc. UIST 2004*: ACM Press (2004) 217–226.

[123] MacLean, A., Young, R.M., Bellotti, V. and Moran, T.P. Questions, Options, and Criteria: Elements of Design Space Analysis. *Human-Computer Interaction (HCI) Journal*, 6, 3&4 (1991) 201–250.

[124] MacLean, A., Young, R.M. and Moran, T.P. Design Rationale: The Argument Behind The Artifact. *Proc. CHI 1989*: ACM Press (1989) 247–252.

[125] Mankoff, J., Dey, A.K., Hsieh, G., Kientz, J., Lederer, S. and Ames, M. Heuristic Evaluation of Ambient Displays. *Proc. CHI 2003*. Ft. Lauderdale, Florida, USA: ACM Press (2003) 169–176.

[126] Markus, M.L. and Keil, M. If We Build It, They Will Come: Designing Information Systems That People Want to Use. *Sloan Management Review*, 35, 4 (1994) 11–25.

[127] Mayer-Schönberger, V., *Generational Development of Data Protection in Europe*, in *Technology and Privacy: The New Landscape*, Agre, P.E. and Rotenberg, M., Editors. The MIT Press (1998) 219–241.

[128] Melenhorst, A.S., Fisk, A.D., Mynatt, E.D. and Rogers, W.A. Potential intrusiveness of aware home technology: Perceptions of older adults. *Proc. Human Factors and Ergonomics Society 48th Annual Meeting*: HFES Press (2004) 266–270.

[129] Milardo, R.M. Comparative methods for delineating social networks. *Journal of Social and Personal Relationships*, 9 (1992) 447–461.

[130] Moran, T.P., Chiu, P., Harrison, S., Kurtenbach, G., Minneman, S. and Melle, W.v. Evolutionary Engagement in an Ongoing Collaborative Work Process: A Case Study. *Proc. CSCW 96*. Boston, MA, USA: ACM Press (1996) 150–159.

[131] Müller, G., *Presentation at "Privacy In Context" workshop at the Ubicomp 2005 conference.*: Tokyo, Japan (2005).

[132] Müller, G. and Rannenberg, K., Editors, *Multilateral Security in Communications, Volume 3: Technology, Infrastructure, Economy,* Addison Wesley: München (1999) ISBN: 3-8273-1426-7.

[133] Nagel, K., Hudson, J. and Abowd, G.D. Predictors of availability in home life context-mediated communication. *Proc. CSCW'04*: ACM Press (2004) 497–506.

[134] National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12 (1996). Available from: http://csrc.nist.gov/publications/nistpubs/index.html. Last accessed: last visited 4/10/2005.

[135] Nielsen, J. *Usability Engineering*, Academic Press: Boston, MA, USA (1993) ISBN: 0125184050.

[136] Nielsen, J. and Mack, R.L., Editors, *Usability Inspection Methods*, John Wiley & Sons: New York, NY, USA (1994) ISBN: 0-471-01877-5.

[137] Norman, D. *The Design of Everyday Things*, Currency (1990) ISBN: 0385267746.

[138] Norman, D. *The Invisible Computer*, MIT Press (1999) ISBN: 0262640414.

[139] Norman, D.A. and Draper, S.W., Editors, *User Centered System Design: New Perspectives on Human-Computer Interaction*, L. Erlbaum Associates: Hillsdale, NJ, USA (1986).

[140] Norris, C. and Armstrong, G. *The maximum surveillance society: The rise of CCTV*, Berg: Oxford, England (1999) ISBN: 1-85973-226-7.

[141] Northrop Grumman Corp. *TRIMARC - Automatic Incident Recording System*. (2002). Available from: http://www.trimarc.org/perl/about_trimarc.pl and http://www.nascio.org/scoring/files/2002Kentucky7.doc Last accessed: 4/2/2004.

[142] Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980). Available from: http://www.oecd.org

[143] Palen, L. and Dourish, P. Unpacking "Privacy" for a Networked World. *Proc. CHI 2003*: ACM Press (2003) 129–136.

[144] Patrick, A.S. and Kenny, S. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. *Proc. PET 2003*, LNCS 2760: Springer Verlag (2003) 107–124.

[145] Patton, J.W. Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology*, 2 (2000) 181–187.

[146] Pilu, M., *Image capture method, device and system*. Hewlett-Packard Development Company, L.P. United States Patent No. 20040202382 (2004).

[147] Povey, D. Optimistic Security: A New Access Control Paradigm. *Proc. New Security Paradigms Workshop*. Ontario, Canada: ACM Press (1999) 40–45.

[148] President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization, Report to the President* (2005). Available from: http://www.nitrd.gov. Last accessed: 3/22/2005.

[149] Privacy & American Business Consumer Privacy Attitudes: A Major Shift Since 2000 and Why. *Privacy & American Business Newsletter*, 10, 6 (2003).

[150] Radio-Television News Directors Association, *Hidden Cameras, Hidden Microphones: At the Crossroads of Journalism, Ethics and the Law* (1998). Available from: http://www.rtndf.org/

[151] Rannenberg, K. Identity Management in mobile cellular networks and related applications. *Information Security Technical Report*, 9, 1 (2004) 77–85.

[152] Rannenberg, K. Multilateral Security: A Concept and Examples for Balanced Security. *Proc. New Security Paradigms Workshop*: ACM Press (2000) 151–162.

[153] Rannenberg, K. Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for Multilateral Security. *Proc. Security and Control of Information Technology in Society – Proceedings of the IFIP TC9/WG 9.6 Working Conference*. Onboard M/S Ilich and ashore at St. Petersburg, Russia: North-Holland, Amsterdam (1993) 113–128.

[154] Robinson, P. and Beigl, M. Trust Context Spaces: An Infrastructure for Pervasive Security in Context-Aware Environments. *Proc. Security in Pervasive Computing 2003*, LNCS 2802: Springer Verlag (2004) 157–172.

[155] Samuelson, P. Privacy As Intellectual Property? *Stanford Law Review*, 52 (2000) 1125.

[156] Sasse, A. Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. *Proc. 2003 Workshop on Human-Computer Interaction and Security Systems at CHI 2003* (2003).

[157] Schneier, B. *Secrets and Lies: Digital Security in a Networked World*, Wiley Computer Publishing: New York, NY, USA (2000) ISBN: 0-471-25311-1.

[158] Smith, I.E., Consolvo, S., Hightower, J., Hughes, J.I., Iachello and LaMarca, A. Social Disclosure Of Place: From Location Technology to Communication Practice. *Proc. 3rd International Conference on Pervasive Computing*, LNCS 3468. Munich, Germany: Springer Verlag (2005) 134–151.

[159] Som, C., Hilty, L.M. and Ruddy, T.F. The Precautionary Principle in the Information Society. *Human and Ecological Risk Assessment*, 10 (2004) 787–799.

[160] Stajano, F. *Security for Ubiquitous Computing*, John Wiley & Sons (2002) ISBN: 0470844930.

[161] Suchman, L.A. *Plans and Situated Actions - The problem of human machine interaction*, Cambridge University Press (1987).

[162] Sweeney, L. k-anonymity: A Model For Protecting Privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10, 5 (2002) 557–570.

[163] Swiss Federal Data Protection Commissioner, *7. Tätigkeitsbericht 1999 / 2000 (7th Annual Report 1999/2000)* (2000). Available from: http://www.edsb.ch/

[164] Terrell, T. and Jacobs, A. Privacy, technology, and terrorism: Bartnicki, Kyllo, and the normative struggle behind competing claims to solitude and security. *Emory Law Journal*, 51, 4 (2002) 1469–1511.

[165] The Yankee Group, *2004 Mobile Users Survey* (2004). Available from: http://www.yankeegroup.com

[166] Townsend, M. and Harris, P., *Security role for traffic cameras: London's new charging zone helps to form 'ring of steel' guarding capital against al-Qaeda bombers*, The Observer, 2/9/2003.

[167] Tran, Q.T., Calcaterra, G. and Mynatt, E. Cook's Collage: Deja Vu Display for a Home Kitchen. *Proc. Home Oriented Informatics Telematics 2005*. York, UK (2005) 15–32.

[168] Truong, K.N. and Abowd, G.D. INCA: A Software Infrastructure to Facilitate the Construction and Evolution of Ubiquitous Capture & Access Applications. *Proc. Pervasive 2004*, LNCS 3001. Linz/Vienna, Austria: Springer Verlag (2004) 140–157.

[169] Truong, K.N., Abowd, G.D. and Brotherton, J.A. Who, What, When, Where, How: Design Issues of Capture & Access Applications. *Proc. Ubicomp 2001*, LNCS 2201. Atlanta, GA, USA: Springer Verlag (2001) 209–224.

[170] Truong, K.N., Patel, S.N., Summet, J. and Abowd, G.D. Preventing Camera Recording by Designing a Capture-Resistant Environment. *Proc. Ubicomp 2005*, LNCS 3660. Tokyo, Japan: Springer Verlag (2005) 73–86.

[171] UK Information Commissioner, *CCTV Code of Practice* (2000). Available from: http://www.informationcommissioner.gov.uk/

[172] 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* (1973).

[173] United States General Accounting Office, *Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, D.C.*, GAO-03-748, General Accounting Office (2003). Available from: http://www.gao.gov/cgi-bin/getrpt?GAO-03-748. Last accessed: 3/21/2006.

[174] US Department of Health and Human Services, Health Insurance Reform: Security Standards; Final Rule, *45 CFR Parts 160, 162, and 164*.

[175] Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27, 3 (2003) 425–478.

[176] Want, R., Hopper, A., Falcão, V. and Gibbons, J. The Active Badge Location System. *ACM Transactions on Information Systems*, 10, 1 (1992) 91–102.

[177] Wardell, J., *LexisNexis Breach May Be Worse Than Thought*, AP Financial Wire, 4/13/2005

[178] Weiser, M. Some Computer Science Problems in Ubiquitous Computing. *Communications of the ACM*, 36, 7 (1993) 75–84.

[179] Westin, A.F., *Harris-Equifax consumer privacy survey 1991*, Equifax Inc., Atlanta, Georgia (1991).

[180] Westin, A.F., Editor *Information Technology in a Democracy*, Harvard University Press: Cambridge, MA, USA (1971).

[181] Wheeler, L. and Rois, H.T. Self-Recording of Everyday Life Events: Origins, Types, and Uses. *Journal of Personality*, 59, 3 (1991) 339–355.

[182] Whitten, A. and Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proc. 8th USENIX Security Symposium*. Washington, DC (1999) 169–184.

[183] Wynekoop, J.L. and Conger, S.A. A Review of Computer Aided Software Engineering Research Methods. *Proc. IFIP TC8 WG 8.2 Working Conference on The Information Systems Research Arena of The 90's*. Copenhagen, Denmark IFIP (1990).

[184] Zarski, T.Z. "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 & Technology*, 5, 2002/2003 (2002) 1–54.

[185] Zero-Knowledge Systems. *The Freedom Network Architecture (Version 1.0)*. Available from: http://www.zks.net/products/whitepapers.asp. Last accessed: 1/1/2000.

[186] Zetter, K., *CardSystems' Data Left Unsecured*, Wired News, 6/22/2005.

[187] Zurko, M.E. and Simon, R.T. User-Centered Security. *Proc. New Security Paradigms Workshop*: IEEE Press (1996) 27–33.

VITA

GIOVANNI IACHELLO

Giovanni Iachello was born in Torino (Italy) in 1974. He studied Informatics Engineering at Padua University (Italy). After graduating in 1999, he worked for Altoprofilo SPA, a firm providing corporate IT consulting services, in the fields of security management, personal data protection and mobile 3G applications. In 2002, he joined the Computer Science PhD program at Georgia Institute of Technology. In 2004, he worked for Intel Research in Seattle (WA, USA), on the development and deployment of a location-enhanced messaging system.

In 2003–2004, he was Fellow of the Sam Nunn Security Program funded by the MacArthur Foundation, focusing his research on the security management of ubiquitous computing applications. He is member of ACM, IEEE, IFIP WG9.6/11.7 “IT-Misuse and the Law” and SIGCHI.

When not writing his thesis, he enjoys all things Alpine: hiking, biking, skiing, snowshoeing and swimming.