Conceptions of Trust: How Designers Approach Usable Privacy and Security

Colin Birge

A dissertation

submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

University of Washington

2013

Reading Committee:

Beth Kolko, Chair

Jennifer Turns, Co-Chair

Mark Zachry

Program Authorized to Offer Degree:

Human Centered Design & Engineering

University of Washington

Abstract

Conceptions of Trust: How Designers Approach Usable Privacy and Security

Colin Birge

Chair of the Supervisory Committee:

Professor Beth Kolko and Professor Jennifer Turns

Human Centered Design and Engineering

Designers who create user interfaces are frequently required to ask users for personal information. For the user, this is a "trust question": Do I, the user, trust the system or entity that is asking me for this information? The creation and management of these trust questions is an important aspect of the research field called usable privacy and security. However, most working designers do not focus exclusively on usable privacy and security problems. Decomposition and modularity of trust and usable privacy and security issues are problematic for working designers.

Studies in the usable privacy and security field have traditionally focused on the usability of specific interface elements, or on a specific usable privacy and security problem. This dissertation explores how designers approach and handle these trust questions in their design process. A multi-modal study investigates how designers conceive of usable privacy and security in their daily work. The object of study is a working designer for whom privacy and security is not a primary task in their daily job. The study uses a survey based on a snowball sample of professional design online forums and semi-

structured interviews to explore the attitudes and conceptual models of designers who produce designs involving “trust questions.”

The results showed that working designers are interested in usable privacy and security issues but often have problems decomposing and modularizing the problem space of usable privacy and security. Usable privacy and security problems are seen as important in the abstract but are hard to identify and engage as part of day-to-day work. To reach the shared goal of making it easy for working designers to achieve positive usable privacy and security outcomes including an increased sense of user satisfaction and safety, it will be important for the research community to find ways to assist working designers with that decomposition and modularization process.

Table of Contents

Table of Contents 1

List of Tables 5

Acknowledgements 7

Dedication 8

Chapter 1: Setting the Scene 9

Introduction 9

Background 11

Trust Interactions and Trust Decisions 14

The Role of Designers 16

The Attitudes and Needs of the Designer 19

Methodology 20

Organization 21

Chapter 2: Literature Review 23

Introduction 23

Social Construction of Trust and Security 24

Theory and Trust 28

Situated Action *31*

Activity Theory *33*

Trust *36*

Ethics *38*

Satisfaction and Anshin *40*

Usable Privacy and Security Studies 42

Whitten & Tygar *42*

Usability *45*

Adams & Sasse *46*

Experience Studies *47*

Information Security *49*

Privacy *49*

Insights 51

Design and Designers 53

Design Studies 54

Modularity *56*

Summary 58

Research Questions 59

Object of Study 61

Survey 61

Demographic Questions *65*

Role & Employer 67

Age & Gender *69*

Experiential Results 69

Design Study 76

Chapter 4: Survey Results 82

Experiential Results 82

Audiences & Designs *82*

Trust Questions *85*

Details of Design Problem *85*

Design Challenges *89*

Technical Challenges *89*

Stakeholder Concerns and Business Strategy *91*

Compliance *92*

Organization Size and Challenges *93*

Emotion of the Users *94*

Summary of Experiential Data *99*

Resources Used 99

Demographics 101

Role *101*

Experience Level *102*

Forums *103*

Organization Size *104*

Age *106*

Gender *107*

Reliability 107

Summary 108

Chapter 5: Interview Results 110

Demographics 110

Themes 112

Defining the Problem Space 113

Defining Audience 116

Trust 119

Security 122

Decomposition 126

Synthesis 129

Chapter 6: Conclusion 133

Problem Space and Audience 133

Decomposition and Modularity 138

Trust Questions 140

Future Work 142

Future Implications for Practice 143

Conclusion 144

References 146

Appendix A: Survey request 162

Appendix B: Survey protocol 163

Appendix C: Interview protocol 172

List of Tables

TABLE 1: TYPICAL AUDIENCES FOR DESIGNERS. 82

TABLE 2: NUMBER OF AUDIENCE CATEGORIES SELECTED BY DESIGNERS 83

TABLE 3: TYPICAL DESIGN TYPES CREATED BY DESIGNERS 84

TABLE 4: NUMBER OF DESIGNERS WHO WORKED ON A TRUST QUESTION 85

TABLE 5: TYPE OF DESIGN PROJECT IDENTIFIED BY DESIGNERS 86

TABLE 6: INTENDED AUDIENCE FOR DESIGN PROJECT 86

TABLE 7: TYPES OF INFORMATION COLLECTED 87

TABLE 8: PROBLEM COMPLEXITY SELF-RATING 88

TABLE 9: RESOURCES USED 100

TABLE 10: EXAMPLE PHRASES FROM PROFESSIONAL TITLES 101

TABLE 11: DURATION OF POSITION 102

TABLE 12: DURATION OF TIME IN PROFESSION 102

TABLE 13: PARTICIPANTS IN FORUMS 104

TABLE 14: APPROXIMATE SIZE OF CURRENT EMPLOYER 105

TABLE 15: CONSULTANT / SELF-EMPLOYED ORGANIZATION SIZE 105

TABLE 16: OTHER UX DESIGNERS' ORGANIZATION SIZE 106

TABLE 17: PARTICIPANT AGE DISTRIBUTION 106

TABLE 18: AGE GOODNESS-OF-FIT TEST 107

TABLE 19: DEMOGRAPHICS OF INTERVIEW PARTICIPANTS 110

Acknowledgements

Thanks to my committee: my chairs Beth Kolko and Jennifer Turns, and Mark Zachry. Thanks also to David Hendry, Jacob Wobbrock, David LeBlanc, Dennis Wixon, Lee Baxter, Julie Lorah, and Michele Poff.

I could not have finished this work without my family, especially: Lynn Weber-Roochvarg; Alan Roochvarg; Edward Birge; and my grandfather, Edward A. Birge.

Special thanks to Rebecca Walton, Kathryn Mobrand, and Jerrod Larson. My thanks also to Peg Achterman, Cameron Birge, Kathleen Brennan, Larry Brennan, Malabika Ghosh, Kathleen Gygi, Kristen Harbeson, Tabitha Hart, Chris Keroack, Laura Osburn, Jennifer Page, Elly Searle, and Maarten van Dantzich. At UBC, thanks to Jennifer Burns, Paul Hobson, Eunice MacCharles & Doris Yen.

Holly shares the world with me every day. I'm forever grateful.

Colin Birge

Vancouver, British Columbia

Dedication

In memory of Edward A. Birge, M.D.

Chapter 1: Setting the Scene

Introduction

As I type these words, I am sitting in a Seattle coffee shop. My laptop is connected to an open Wi-Fi network provided for customers. Using a simple, freely available Mozilla Firefox add-in called Firesheep [Butler 2010], I can scan the Wi-Fi network traffic for customers who've logged in to their favorite web sites insecurely. When the add-in was first released in October of 2010, it was possible to use the add-in to log into major web sites such as Facebook.com under another user's account.

Why would anyone use such an insecure system? This is a deceptively complex question that I will examine at much further length, but for the sake of discussion, let us consider the notion of "convenience." Users appreciate the convenience of being able to check their favorite web sites & e-mail at their local coffee shop. It is a model that is simple, flexible, and easy to use.

One could, of course, imagine a more secure model. Some coffee shops use more advanced Wi-Fi technology such as WEP security and SSL to make it more difficult for a malicious party to "listen in" to the Wi-Fi network traffic. However, this requires several extra steps. The coffee shop administrator must establish a password (or passwords), which each customer then has to enter into his or her own system. Under some systems, the user must open a web browser and accept a small security token from the router to be allowed to use the local Wi-Fi. This takes time and a correctly configured system. If anything goes wrong with the router security, or if the customer has issues with obtaining the security token or password, does the barista pulling a shot have the time or the expertise to diagnose and fix the problem? Or might the Wi-Fi simply become unusable? The potential complexities with a secure system often lead to the use of un-secured Wi-Fi.

Open Wi-Fi networks are a classic and well-researched example of the tension between usability and security. Usability principles suggest that the open Wi-Fi network is appropriate. It is, by far, the easiest type of Wi-Fi network to set up, and users can gain access without any additional steps. For security professionals, however, it opens up considerable risks to computers and data.

Another, related example: Consider the question, "Enter your username and password." What are you, the user, being asked here? Most simply, this is an authentication question: please prove that you are you. This question uses what's called single-factor authentication: something you know (your password) matched with your user name (your unique identifier).

A password dialog serves several purposes, but it is at heart a trust interaction. The interaction is between the system and the user. You, the user, must determine whether you trust the system enough to pass along your credentials, given the risk that those credentials can be exploited. The system must trust that you, the user, are who you say you are and can be trusted with your access permissions.

There are several threats inherent in this interaction, however. Again, consider that open Wi-Fi network. When we suggest that you, the user, must determine whether you trust "the system," it is not enough to say that you trust the entity — web site, operating system, etc. — that is asking you for your password. You must also determine whether you trust the *network* that you are using to access that system. Perhaps you trust your e-mail provider, but do you trust the open Wi-Fi network that you're using to send your password to that e-mail provider?

Another threat is known as *phishing*. The password dialog from your e-mail provider looks familiar. However, someone who is phishing—i.e., looking to steal your identification for their own purposes—asks exactly the same question in exactly the same way. The phisher's purpose is more sinister: they want to replace one party in the trust interaction with themselves.

From these examples, I hope to illuminate two points. First, there is a complex and tightly woven interaction between security and usability of an interactive system, and by extension the user experience.

That interaction has a direct impact on maintaining the security and privacy of a user's data and personal information. This problem space goes by several names, but I will follow the lead of Lorrie Faith Cranor and others by calling it "usable privacy and security." Second, much of the interaction between usability and security is based on the multi-faceted notion of *trust*: how a system trusts a user, how the user trusts the system, and what information is exchanged between the two.

As we will see, usable privacy and security is a fast-growing area of research. In this introduction, I will briefly describe the current state of the usable privacy and security field, explain the research questions I have chosen to explore within it, and discuss the structure of this dissertation.

Background

The study of digital information security is nearly as old as computer science itself, but the related discipline of providing usable solutions to information security issues has matured only in the last twenty years.

Saltzer and Schroeder [1975] is usually acknowledged as the first published paper to call for inquiry and development of usable privacy and security. It was written as a general summary of digital information security principles as they were understood at the time. One of those principles was stated as follows:

> It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.

Despite this call to action, little work was published on usable privacy and security principles for over a decade [Cranor and Garfinkle 2005]. The study of the "psychological acceptability" of systems took on new life in the 1980s, with foundational studies by Card and Newell [1985], Norman and Draper

[1986], Suchman [1987], Gaver [1991] and others. This early research into usability rarely touched on issues of digital information security and privacy, however.

What we might call the "modern era" of usable privacy and security research began with the publication of two important papers in 1999: Whitten & Tygar's "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" [1999] and Adams & Sasse's "Users Are Not The Enemy: Why Users Compromise Security Mechanisms And How To Take Remedial Measures" [1999]. Both of these papers strongly influenced the design of this project, and I will discuss them at length in my literature review. For now, it suffices to note that these papers set a standard followed by most research in the field to this day: studies of user attitudes and behavior driven by a mix of qualitative and quantitative studies with the user as the direct object of study.

Because the discipline of usable privacy and security is so new, to date there have been few attempts to draw boundaries around it—to say, "this is a usable privacy security study." The study of usable privacy and security is at the intersection of several related fields: trust, information security, privacy and governance, sociology, and user-centered design.

Central to all of these approaches is the assumption that, to paraphrase Adams & Sasse [1999], users are in fact *not* the enemy, but indeed are key to preserving the security and privacy of their data. For those with a usability background, this may seem like a blatantly self-obvious observation, but many security practitioners to this day believe otherwise. Common security models such as password security, access control lists, and the principle of least privilege are based on the "need to know" principle, adapted from the military. In this conceptual model, users are to be trusted only with the least amount of information and access they require in order to complete their task. More knowledge leads to more potential leaks. The problem, of course, is that without sufficient knowledge of the implications of their actions, users can and often do make mistakes that imperil the security of their information. [Adams and Sasse 1999]

If the usable privacy and security discourse community can be defined as a set of researchers and practitioners working from a shared set of assumptions and terminology across a range of fields of study, where does this research study fit in? To the list of related objects of study described above, I would add more: the study of how *designers* approach usable privacy and security.

Let me be clear about my use of the term "designers," which is often overloaded with meaning. I use "designer" to mean the people who define the user interaction of a system: the text, graphics, features, conceptual models, user flow, and user interaction. These designers may work in a variety of contexts: web sites, mobile devices, mapmakers, designers of physical spaces such as zoos and theme parks, and more. I use the term in its sense of an HCI practitioner: an interaction designer or software architect or usability specialist or developer who creates the interface or model for a user interaction. This is a deliberate departure from the more traditional design community definition of a designer as someone who has been formally trained and/or has extensive experience in a design discipline. Unfortunately, there is no evidence to suggest that only designers with formal training create interfaces with trust implications. Nor is there any reason to believe that such formally trained designers will exclusively create interfaces with trust implications in the future.

Of course, not every designer works in fields that require their users to give up aspects of their privacy. Most do not. An architect is a designer of user experience, in a way, but the only privacy that the architect concerns himself or herself with is the physical privacy of the space. (Which is, to be clear, a real and complex problem, but outside the scope of this discussion.)

We can further define our interest, then. It is not solely user experience designers that are of interest in this study, but user experience designers who must, with no malice, intrude upon a user's privacy.

Trust Interactions and Trust Decisions

A key idea in usable privacy and security literature is the concept of "trust," another overloaded term. Chapter Two will describe the rich history of the literature in trust in more detail, but briefly, researchers have identified several key elements in the notion of trust. First, trust involves a relationship or interaction between two parties. Second, trust happens in the absence of control on the part of one or both parties - meaning, each party in the trust interaction does not have full control over the actions of the other party. Third, trust is the *subjective* measure by one party of the probability that the second party will perform the desired action. Trustworthiness is the pattern of that subjective measure over a period of time. [Cofta 2007; Gefen 2002; Patrick et al. 2005]

Trust is achieved through communication between two or more parties. A level of trust (or lack of trust) is intrinsic in how any communication is sent or received [Cofta 2007]. That trust has been described as a social interaction between the truster and the trusted, even if the "trusted" is a system rather than an individual [Nissenbaum 1998].

How, then, is that social interaction created? It occurs when one person makes a decision to trust another party, a "trust decision." The decision point is when the person decides that in the context of their current interaction, they trust the other party to perform the actions they expect. You might trust your bank to preserve your money and give it to you upon request, for instance.

Trust decisions are commonplace in life and often unconscious. If you walked into a bank and talked to a teller, the trust interaction would use social as well as technical cues. You are in a bank; the teller is dressed professionally and seated behind the desk; therefore you trust that the bank teller is in the role they claim to be. In the case of an online trust interaction, however, the only cues that you have are in the user interface. It is for that reason that the study of trust interactions in user interfaces is important for creating a robust information security model.

When you use the open Wi-Fi at a coffee shop, you are making an implicit trust decision. You are trusting that either no one present has the technical knowledge to intercept your communications or if they do, they will not misuse the information they collect. Individuals with data security training, more aware of the risk, are typically more horrified by this trust decision than the average user [Klasnja et al. 2009]. For many, convenience trumps the potential harm, if they are indeed aware of the potential harm at all.

Trust interactions also occur in person-to-person communications online. Consider eBay, the auction online site, which can also be described as a platform for connecting buyers and sellers together. Again, one participant is forced to rely on UI cues to determine whether the person on the other end of the transaction is trustworthy. eBay uses specific UI cues to help show an individual's "reputation": how many times the individual has used the site, what feedback they've received, and more. Again, though, the decision on bidding or accepting bids on the site becomes a trust decision, supported by the UI cues provided by the web site.

Similarly, in social networks and virtual communities, users must choose how much personal information they want to share, and with whom. This is a trust decision: whom do I know who can be trusted, and with what information? Services such as Brightkite and Google Latitude, for example, allow the user to share information about their current location, but that information carries physical security risk. For example, an attacker could determine that you're away from your home and use that time to rob your house. More subtly, a trusted person (your partner) may not be trusted at all times with information about your current location (because you're at the jewelry store shopping for a gift). Both services require carefully thought-out UI to provide the user with a clear choice in deciding who should receive the information about your location, and when that information should be shared. This, too, is a trust decision.

Trust decisions are a key element of this research. They are a focal point for trust and a lens through which we can evaluate how trust interactions occur. Designs that support trust decisions must ask the user a *trust question.* A trust question can be summarized very simply. "Do you, the user, trust this system or entity with the information requested?" Trust questions are not usually explicit; rather, they are implicit in the request made by the system for input of personal or private information.

The Role of Designers

The notion of trust interactions between users and systems is well explored and has been studied many times [Riegelsberger and Vasalou 2007]. An inherent assumption of every trust interaction in HCI is that it is a *designed* interaction: a designer has created the user interface that allows the system to decide whether it trusts the user and the user to decide whether to trust the system. Trustworthiness intrigues HCI practitioners because the trust interaction is, in some ways, an artificial creation.

Because the interaction between the user and the system is mediated through the user interface, the interface designer has a great deal of influence over the trust decisions that the user makes. This influence can show itself in obvious or subtle ways. Google's search engine, for example, will show a warning when one of its search results is suspected as a site designed to steal information or install malware from a user. This warning is obvious: do not trust this site. More subtle indicators include a "lock" symbol or a green address bar in a browser, indicating that a safe, encrypted connection has been established. This notice is subtler: this connection is secure; you can trust the connection with your sensitive information. Of course, the subtler the interface design, the more user knowledge is required to interpret it correctly, and the more likely the design is to fail. (See, for example, the mixed results of "privacy indicators" in web browsers [Egelman et al. 2009].)

Historically, information security professionals have tended to regard designers with some skepticism. A common trope in the information security field is that security and usability are inversely

proportional: the more usable a system is, the less secure it is [Yee 2005]. "Any user interface can be spoofed [i.e. imitated for malicious purposes], so what's the point of creating a secure user interface?" one self-described hacker asked me. Yet interface design can have a major positive or negative impact on the overall security of a system. For example, security measures that harm usability can remain unused [Whitten and Tygar 1999] or create extra design clutter for relatively little gain [Wu et al. 2006]. To create usable systems that preserve security and privacy, the design community needs to be engaged in ways that are useful, thought provoking, and contextual.

This study focuses on the design practices of usable privacy and security. Design practice studies often focus on the decisions made by the designer in the course of their process of exploration and iteration [Dorst 2008, Goel and Pirolli 1992]. Among many other concepts, these decisions can include defining the proposed scope of the design, the design's intended audience, and the "structure" or "flow" of the design.

In the research world of usable privacy and security, an ever-increasing body of literature now exists on how users work with trust interactions. However, the organizational process used in creating trust decisions and the designer's work practices in crafting trust interactions are both less explored.

Consider the following dilemma. As noted earlier, a general principle in information security is to restrict or reduce functionality when it is not needed. This is called *reducing the attack surface*, and is conceptually similar to the "need to know" principle. For example, if a web site has malicious code hidden in JavaScript, the attack will not work if the user's web browser has JavaScript turned off.

Of course, this line of logic can be taken too far. (A common joke in the information security field is that "The most secure system is the one that is not plugged in.") As more features are restricted for security reasons, the system becomes harder and harder to use. How, then, does the designer decide which features should be restricted, and when and how those restrictions should be lifted?

As a designer, one way to frame the problem is to ask yourself this question: *How much do I trust the user not to do harm?* If the user can be trusted with a rich feature set, then there is no need to place restrictions on those features. On the other hand, less trusted users with greater data protection requirements might need a reduced attack surface for their own security.

Notice that the question is about the user *doing harm*, not *the user doing harm to their data*. One common response to the question is this: if the user chooses to do something potentially harmful to their own data, is that not their own lookout? But this question is dangerously reductive, because it ignores the potential of harm to the rest of the network of information systems. User interfaces are a mode of interaction between a user and the full architecture of a network to which they have access, not just their own system. For example, consider the user whose computer has been compromised by a malicious web site. Not only is their own data now compromised, but the user's computer can be turned into part of a *zombie network*, a series of compromised computers with malicious code designed to silently and simultaneously launch attacks against third parties.

Consider, then, the theoretical and practical implications of these questions. Should the system allow all functionality to run without restriction? (And does this pose an ethical dilemma for the designer?) Should the system ask the user before enabling potentially dangerous features? If the system should ask the user, when is the right time to ask?

In another context, consider the problem of social networks. Designers of such networks typically have strong business and usability reasons to encourage users to share as much information as possible. But how much information is too much?

My research questions investigate how designers approach these issues.

The Attitudes and Needs of the Designer

There are several attempts in the literature to give guidance or tools that designers can use to provide better, more usable interfaces that deal with security and privacy issues. (Examples include guidelines for designers [Patrick, Briggs and Marsh 2005] and the creation and analysis of security patterns [Muñoz-Arteaga et al. 2009].)

However, few of these studies have attempted to systematically describe the specific requirements of designers who work in the privacy and security space. For example, in the design process, when does the designer approach security and privacy concerns? What is the level of designer awareness of user-centered security issues? Is user-centered security seen as a late-stage set of requirements to be met or an integrated part of the full design process?

Also, there is a level of organizational and technical meta-analysis required here. One of the primary constraints on the designer is the technical capability and limitations of the system in providing a secure environment. How much awareness do UI designers have of the technical limitations of their system, and how do they work around those limitations in their interface designs?

I hypothesize that most experienced designers will consider usable privacy and security issues when they are building an interface that has security implications. However, there is limited data available on the tools that designers use, the assumptions that designers make, and the processes that designers follow when working on interfaces that must help users preserve the privacy of their data.

This part of the study is necessarily exploratory. With a limited literature on the practices of usable privacy and security interface designers, the follow-up steps will not be clear until after some initial data is collected. Generally, there are three broad questions to be answered:

1. Fogg [2002] notes that trust questions, which fall under the umbrella of what he calls "persuasive technology," work best when the problem space is narrowly defined and the audience is already receptive. For these designers, how do they define their problem space and their audience?

2. Using the terminology and theoretical framework of Goel & Pirolli [1992]: how do designers structure their approach to the design problem of trust questions, and how do they create modularity and decomposability of these problems?
3. How do designers conceptualize the problem of trust questions in relation to the overall design problem space in which they are engaged?

Methodology

To address these questions, I used an open-ended study with survey and interview data to investigate (in Dorst's words) the actor, the context, and the structure and dynamics of the design approach to trust questions. For this approach, I am indebted to the theoretical framing of Goel & Pirolli [1992], Dorst [2008], and Zimmerman et al. [2007], as well as discussions with Cynthia Putnam [Putnam 2010]. Werlinger et al. [2009] have taken a similar approach to observing the interactions of security IT professionals with their organizations. I will briefly discuss this approach here, with more details to follow in chapter 3.

I began by administering a survey, designed to reach as many designers in as many contexts as possible, constructed to answer two major questions:

1. Who are the actors (designers, organizations) who are working on user interfaces involving trust questions? What context to these designers work in?
2. What examples exist of usable privacy and security issues and trust questions that these designers have seen in their work?

An additional purpose of the survey was to identify and recruit designers who were willing to participate in a future stage of the study.

After the survey was complete, I performed a series of in-depth interviews with designers who were recruited through the previous surveys. These interviews were semi-structured, intended to probe the

problem space of the designer as well as the structured approach, modularity and decomposability of their design problems. The interviews were recorded and transcribed.

The surveys allowed me to identify "wicked" problems in designing trust decisions and other user experiences for usable privacy and security. (I use the term "wicked problem" in the sense of a problem difficult to solve because of contradictory requirements or complex interdependencies. Many usable privacy and security problems fall into this category.) Each interview subject was asked to recall a "wicked problem" in designing a trust decision or other trust user interface from his or her previous work.

The interview data was coded using a grounded-theory approach with checks for inter-rater reliability.

Organization

The remainder of this dissertation is organized as follows:

In Chapter Two, I will review the theoretical framework used for this research, as well as the methodological and epistemological sources that form the background for this study. As usable privacy and security is itself a relatively new field at the intersection of several related discourse communities, I will also give a brief survey of the literature in the field.

In Chapter Three, I will describe the methods used to gather the data for this study.

Because this study is framed using a mixed-methods approach, the results are divided into two chapters. Chapter Four covers the demographics of the respondents and the results of the survey. Chapter Five analyzes the feedback I received from the semi-structured follow-up interviews of a subset of the survey participants.

Chapter Six concludes the dissertation with some overall notes on the findings and contribution of the study, as well as suggestions for future work.

The heart of this study lies at the intersection of several fields of thought and research: design studies, human-computer interaction, information security, and trust and ethics. To begin the discussion, in the next chapter I will place my work in the context of this cross-disciplinary approach.

Chapter 2: Literature Review

Introduction

In the first chapter, we saw that the usable privacy and security discourse community was centered at the intersection of several research traditions: usability, information security, human-computer interaction, trust, ethics, and rhetoric.

One of the challenges of a discourse community that borrows from so many traditions is in creating a coherent story from the research literature, a way to think about the research in this field. Literature on designers and design process is only partly related to literature on human-computer interaction, which is only partly related to more theoretical notions of ethics and social construction. Taken individually, these traditions can be easily understood: together, they can be confusing or even directly conflicting.

In this chapter, I will argue that a way to make sense of this morass is to tell the story of trust. Trust is a powerful concept that emerges in the usable privacy and security literature again and again. Different concepts and constructions of trust provide much of the current, ongoing dialogue in the usable privacy and security field.

When I speak of "trust," what does that concept mean? Trust can be analyzed in mathematical terms, as an equation of subjective probability [Cofta 2007] or as a social interaction between a truster and a trustee [Nissenbaum 2004]. Common to all concepts of trust, however, is the concept of control [Cofta 2007]. Trust must happen when one party in an interaction or relationship does not have full control over the actions of another party. Trust is also contextual: two parties who are choosing to trust each other are doing so in a particular context, with background, history, and reputation all contributing to the decision of whom to trust with how much. [Barth et al. 2006]

Each of these concepts - trust, control, and especially context - needs to be further unpacked to understand the current frame of usable privacy and security research. With that in mind, I will give a brief discussion of how the current conversation about trust has formed, and what lines of inquiry are currently being pursued.

Social Construction of Trust and Security

In analyzing issues of trust and security, one should ask: who *don't* you trust? The answer is in many ways unique to the individual, but as we will see, the answer also is in some ways a social and technologic construction.

Consider the hacker. The term "hacker" itself is somewhat problematic, as many legitimate programmers and engineers embrace the term, preferring its definitions of creative exploration and problem solving [Raymond 2003]. The security community recognizes different classes of hackers, including ethically positive hackers ("white-hats"), hackers who act maliciously and/or criminally ("black-hats") and hackers who act in morally or legally ambivalent ways ("grey-hats"). Some hackers also describe themselves as political activists serving a higher social cause [Still 2005]. I will cover the ethics of hacking and computer security in more detail in the next section, but for now I quote from Luciano Floridi's theories of information ethics [2006]. Hacking, says Floridi, is a breach of privacy and an ethical violation. However, there are times when hacking has an ethical force — a term of art from virtue ethics, meaning a driving force for ethical behavior or an act of a moral agent. For example, when the hacker is working at the invitation of the system owner, or when the hacker is working with the intent of notifying the system owner of potential exploits, the ethical force of the behavior is increased. This is a social construction of hacking.

One early example of the complexity of this social construction was the Sasser worm [Weaver et al. 2003]. Sasser, a malicious "worm" program, was designed to exploit a known Windows vulnerability and

replicate itself via the Internet. The author of the worm, Sven Jaschan, released the program "into the wild" without warning and was later convicted of computer sabotage [2005]. The underlying vulnerability that the Sasser program exploited had been discovered almost six months earlier by Yuji Ukai and Derek Soeder at eEye Digital Security [2004]. Ukai and Soeder were "hacking" Microsoft Windows, looking for vulnerabilities to exploit, but when they found the vulnerability, they immediately and privately notified Microsoft. It was only after Microsoft had released a patch fixing the vulnerability that Ukai and Soeder publicly announced their findings. Ukai and Soeder were considered to be acting as ethical hackers, while Jaschen was considered to be "malicious."

More recently, in early 2013 noted Internet activist Aaron Swartz committed suicide after being threatened with 35 years in jail on what prosecutors described as "hacking" charges. The "hacking" was in systematically downloading academic articles through a campus network to make them public, an action performed without an apparent goal of personal gain [Lessig 2013], and the prosecutor's actions in the case have been widely condemned [Sasso and Martinez 2013]. The social construction of the term "hacker" continues to be problematic.

The motivations of various hackers have been described as "playful" [Turgeman-Goldschmidt 2005], "activist" [Still 2005], "art" and "exploration" [Levy 2001], and "criminal fraud" [Condon and Morrison 2005)]. The disparity of hackers' motivations is as broad as the reactions they create.

One way to describe the social construction of hacking activity divides the type of hacking into "ethical" and "other" activities. The industry security organization EC-Council [2011] created a definition of ethical hacking from which the following list is derived:

Ethical in-group hacking. The ethical in-group hacker is directly engaged or employed by the organization that owns the target systems. He or she is contractually obligated to find exploitable issues with the system and report them confidentially to the organization.

Ethical out-group hacking. The ethical out-group hacker is not directly engaged or employed by the organization that owns the target systems, but nevertheless reports issues that they find in a secure and responsible fashion. In the Sasser example, eEye Digital Security acted as ethical out-group hackers. They were not employed or engaged by Microsoft, but found the vulnerability independently and reported it to the vendor before publishing the vulnerability.

Independent hacking. The independent hacker discloses and discusses exploits publicly, but may or may not notify the vendor and request a fix. They also may or may not use the exploits for personal advantage or gain. In the security community, these are commonly known as "grey-hat" hackers.

Malicious hacking. The malicious hacker does not disclose or discuss exploits publicly, but simply uses the exploits for personal gain or profit. In the process of doing so the malicious hacker may commit legal and/or ethical violations of privacy on one or more systems. In the security community, these are commonly known as "black-hat" hackers. Note that a "black-hat" hacker may in fact be part of an in-group, such as a government or military agency. It is their relationship and communication with the target that defines their status in this social construction.

The boundaries between these categories are rather fluid. Sven Jaschen and Kevin Mitnick are both examples of individuals who moved from one set of behaviors (malicious hacking) to another (independent in-group hacking) [Shimomura and Markoff 1996]. How can we understand those shifts in behavior? And what impact do these behaviors have on the larger community of Internet and computer users?

Boczkowski points out that technological changes and social changes affect each other through a set of mediation processes. These changes are not linear but recursive, meaning that there is a constant back-and-forth process of innovation and change between the social and the technological [Boczkowski 1999].

The computer security community (including all types of hackers and security professionals) has undergone a constant evolution since the 1980s. That evolution, in turn, has had a strong and profound

impact on software technology. Computer users, in turn, have had their role to play. For example, attempts to create strongly secured systems such as Microsoft's Palladium or various operating systems used in military-grade applications have a track record of failing in the broader market, in part due to a negative user reaction to the restrictions inherent in a well-secured system.

Kline and Pinch's description of the Social Construction of Technology (SCOT) model applies here. [1996] SCOT uses "relevant social groups" as objects of study, defined as "those groups who share a meaning of the artifact," and notes that artifacts have "interpretive flexibility," meaning that the same artifact is interpreted differently by different social groups of users.

We have already explored the various groups of hackers, who constitute several relevant social groups for computer security. Let us examine three other groups: vendors, security professionals, and computer users. Vendors are, simply, the vendors who create the user interfaces that other people use. They are typically interested in the security of their products but may not regard security as their sole or core business.

Security professionals are not synonymous with hackers. The security professional is typically concerned with analyzing existing threats and developing countermeasures or mitigations for them. For example, anti-virus vendors such as McAfee are not, typically, hackers in the sense used in this dissertation. Rather, they develop means of detecting existing exploits and providing protections or cleanup measures against those exploits. They do not specifically analyze systems for new security issues; rather, they address security issues that have already been found.

Finally, computer users are most often "customers" of the vendors. Typically, end-users have some level of concern about the privacy and integrity of their data, but expect that software vendors and security professionals will "do the right thing" automatically to protect them. [Nodder 2005] Their knowledge of security issues and willingness to sacrifice functionality for the sake of security is generally

low [Friedman et al. 2002]. End-users may be part of organizations that have specific security policies or directives, enforced by information technology (IT) departments.

These social constructions have an impact on the concept of "information security," one of the core domains of usable privacy and security. Information security can be described as the protection of the information of "computer users" by "security professionals" and "vendors" against threats posed by malicious "hackers." Yet we see that all of these definitions are somewhat fluid, a social construction of a shifting relationship based on technical capabilities, modes of ethics, and security practices. This shifting social construction is one of the elements that should be considered by designers working in the usable privacy and security domain.

Theory and Trust

In Chapter One I gave an introduction to the multi-faceted concept of "trust." For the following discussion, it is useful to grounding that concept in the specifics of a technologic interaction: an interaction between a user and a technology. As such, much of the theoretical and practical research tradition of usable privacy and security is an intellectual descendent of the human-computer interaction (HCI) discipline. It shares many of the same theoretical underpinnings. However, as we will see, the usable privacy and security discourse community heavily relies on certain theoretical frameworks: plans and actions, trust, rhetoric (to a degree), and more. In the following section, I will describe some of the theoretical models that are common to the usable privacy and security community and, by extension, to my own research.

Shneiderman [2002] gave perhaps the best summary of the role that theory plays in research. In his conception, there are five roles, none mutually exclusive. 1. Descriptive theories identify key concepts or variables, and make basic conceptual distinctions. 2. Explanatory theories reveal relationships or processes. 3. Predictive theories, such as Fitts' Law [MacKenzie 1992], make it possible to make

predictions about performance in a range of contexts. 3. Prescriptive theories provide guidelines based on best practice. 5. Generative theories facilitate creativity, invention and discovery.

For the most part, the theories I will discuss in this section are descriptive or explanatory. Their purpose is to help clarify the relationship and the interaction between the two most basic elements in HCI: the human and the computer, or more broadly, the human and any type of technologic interface.

As this dissertation is a project at the intersection of several research fields, so it is also benefits from the work of multiple theorists. In this section, I will discuss the theoretical framework I used in the design and analysis of my study. This theoretical framework includes theories of the *context* of interactions and theories of the *correctness* of interactions, both vital to usable privacy and security.

Early theoretical work in human-computer interaction largely focused around information processing models, a model derived largely from cognitive psychology [Newell and Card 1985; Norman 1991]. In this model, human cognition was enhanced by the use of cognitive artifacts that allowed the user to extend their own information processing capabilities or memory retention beyond normal human limitations. Such artifacts provided a representation of information tailored to the user's requirements. According to this theory, the more closely the representation model (aka conceptual model) mapped to the user's cognitive model (aka mental model), the more usable was the representation and the system.

Two implied assumptions in this model were later challenged by a number of researchers. The first assumption was that the user's interaction with the system could be explored as a single task or interaction, without reference to the broader context of the user's requirements or environment. The second was that human interactions, as with machines, could be analyzed as a set of "plans" with a step-by-step process, when in fact human interactions ranging from personal conversations to work with computers was far more rich and nuanced.

The resulting round of theories has been called "second wave" or "post-cognitivist" human-computer interaction theory [Kaptelinin et al. 2003]. Post-cognitivist theory allows for a discussion, not

just of the individual interaction between a user and a system, but a larger contextual understanding [Gomila and Calvo 2008; Kitzinger 2006]. What is the environment in which the task is being performed? What are the cultural (and in some cases, business) expectations underlying the interaction? Are each user's expectations of the system identical, or would different users of the systems create very different expectations?

It is this post-cognitivist theoretical model that I will use as the primary theoretical basis for my dissertation. Post-cognitivist theories relating to the context of interactions include:

* Situated action. Situated action, a formative theory of human-computer interaction, is heavily referenced by researchers in the usable privacy and security field. Situated action theory helps to explain how trust interactions are situational and a problem of mutual intelligibility, rather than a mere breakdown in a planned interaction model [Suchman 1987].

* Activity theory, viewed through the lens of a designer, reiterates the importance of the *context* of design, focusing especially on the importance of the social and group context of a particular interaction. Activity theory emphasizes the notion of the *goal* of an interaction, and notes that the goal is often within the context of a shared activity rather than a single task. It shares with the situated action perspective the fundamental notion that speaking cannot be detached from acting and that human cognition cannot be separated from this acting. Activity theory uses the interpersonal communication of speech and a focus on human interaction with material objects as a lens for viewing human computer interaction [Kuutti 1996].

* Social Construction of Technology (SCOT) demonstrates that the designer's intent is not always the way that a design is used: technology is socially constructed to adopt new meaning for the user. This construction affects ordinary users as well as the shifting "roles" of users, designers, and hackers in a usable privacy and security context [Pinch and Bijker 1987].

Process is an important object of my study. I hypothesize that the process by which usable privacy and security decisions are made is, for most designers, a small aspect of a larger design process that they must complete in order to fulfill their goals. It is imperative to understand the larger design process in order to understand the context of these usable privacy and security decisions.

In addition to these broader theories that are common to notions of human-computer interaction, usable privacy and security brings ethical and moral questions to bear. Design trade-offs are a part of every human-computer interaction, but in a space where the trade-offs can expose a user to direct harm, the "correctness" of an interaction design must be questioned more rigorously. Theories allowing for discussion of the correctness of interactions include:

* An-shin [Kikkawa et al. 2003], an extension of trust, which looks at the rightness of actions.

* Trust and ethics, described briefly in the introduction. All interactions between users and systems are based on trust, and trust (implicitly or explicitly given, deserved or undeserved) is the heart of every usable privacy and security interaction [Floridi 2006].

It is worth noting that this is not meant to be an exhaustive review of the theories that could potentially apply to human-computer interaction, nor even a full review of the theories that could be used to examine usable security and trust questions. However, as we will see, the combination of the theories described above provides a useful framework for analysis and study of usable privacy and security.

Situated Action

Lucy Suchman's discussion of situated action [Suchman 1987] was, for me, the first step in forming a frame to look at usable privacy and security. Suchman critiqued what she called the "plan model," where "action is a form of problem solving, where the actor's problem is to find a path from some initial state to

a desired goal state, given certain conditions along the way." Her critique, she said, was that plans "are located in the larger context of some ongoing practical activity," and suggested as an alternative the notion of what she called "*situated action*." Suchman laid out five propositions to describe this:

> Plans are representations of situated actions.
>
> In the course of situated action, representation occurs when otherwise transparent activity becomes in some way problematic.
>
> The objectivity of our action is achieved rather than given.
>
> A central resource for achieving the objectivity of situations is language.
>
> Mutual intelligibility is achieved on each occasion of interaction with reference to situation particulars, rather than being discharged once and for all by a stable body of shared meanings.

Suchman's critique of the earlier model, put more simply, was that older cognitive models of communication are problematic once humans are brought into the equation. The computer typically does not have a full representation of the "situation" or context of the action, as a human does. Humans, by contrast, do not formally "plan" an action in the way that a computer does; human actions are often not "objective" and often are not represented in a way that the computer can easily understand.

For the purposes of usable privacy and security, Suchman's analysis suggests a few points. First, it raises issues with the notion of "agents," a goal of some security researchers (e.g. [Cranor 2002]). In this domain, the notion of the agent is the software program that is empowered to make security or trust decisions on your behalf. Suchman might argue that these agents are necessarily problematic, because the agents do not have access to the same contextual and situational information that the human would in the same situation. Without that extra information, the trust decisions made on behalf of the user might be very different than the decisions the user would make themselves, which has significant potential impact for the security and privacy of the user's information.

Second, Suchman's analysis suggests that action is essentially transparent: that is, the "planning" process is not a conscious process of cognition unless something in the interaction breaks down. This is important to designers of trust user interfaces because trust questions are, to varying degrees, an interruption of the user's primary task. They interrupt the user's original situated action and require the user to respond to a query in a different domain.

Suchman might call this interruption a need for "representation." The activity has become problematic. There is a potential for the user's data security to be compromised in some way. More recent usable privacy and security literature has emphasized the importance of limiting these interruptions to the user flow [Johnston et al. 2003] but at what cost? An interface that takes care of everything for the user is essentially acting as an agent, and some of the concerns with user agents have already been identified. Suchman's theory implies a strong need for understanding the needs and goals behind each trust interaction.

Third, Suchman emphasizes the importance of what she calls "situated use of language." She questions the traditional cognitivist viewpoint that there is a "shared store" of language to be drawn upon for recognition and understanding. Interpretation is a constant. The designer's notion of language or symbols may not match the user's, even if both come from the same culture. For usable privacy and security professionals, this is an important observation. There are case studies in the literature of attempts to create a trust interface that failed due to the user's incomprehension of the language used in the security profession (e.g. [de Paula et al. 2005, Whitten and Tygar 1999]). Suchman's theory supports the need for both analysis of context and audience analysis in trust interface design.

Activity Theory

Activity theory is a theoretical framework for analyzing the interaction between a "subject" and the world, derived from principles laid out by Russian psychologists Vygotsky and Leontiev, among others.

The unit of study is the "activity," the purposeful interaction of the subject with one or more "objects," in which "mutual transformations between the poles of 'subject-object' are accomplished" [Nardi 1996]. Between the subject and object are often *mediating artifacts,* described by Engeström as "tools and signs" or artifacts that help to mediate and define the activity between the subject and the object. [Engeström 1999]. Other writers refer to these mediating artifacts simply as *tools*.

A slightly more complex model is described by Kuutti [1996], who adds the *contextual* elements of "community," "rules," and "division of labor" into the discussion. The subject is a part of a community of shared objects and potentially shared activities, with rules governing the interaction and the division of labor within the community. Kuutti gives an example that directly shows a design activity:

> Let us take a more contemporary example of an activity – a software team programming a system for a client. The object is the not-yet-ready system which should be transformed into a delivered, bug-free application. The team is the community sharing the object, perhaps joined by some representatives of the customer. There is a certain division of labour: between manager and his or her subordinates, between software developers and user representatives and between the team members. There is a set of rules covering what it is to be a member of this community. Part of these rules may be explicit – set by the laws, parent organization, or the team manager – but part of them is most certainly implicit, either as a part of the general working culture or developed locally during the time when the team has been working together. Some rules may be constructed for this particular project, for example how the user representatives of this particular customer shall be treated. In each step of the transformation process a different set of tools and instruments is used in the transformation process: analysis methods, computers, programming tools, walkthroughs, rules of thumb, etc. The collection of these tools has a history: it is a result of a process of cumulation and rejection at both company and team level and additions and

deletions to it may occur during any project. Whatever the members of the team do during the project is shaped by the context of activity.

Kuutti's model is useful for examining the activities of designers as it provides a theoretical framework for the design activity itself. We should remember that activity theory could be applied to either the activity of creating the design itself or the activity that a design is intended to enable. The actors, objects, tools and contextual elements are different in each case, but the model remains the same.

Activity theory is similar to situated action theory (and different from more traditional cognitive theories of interaction) in that it requires that the scope of analysis be extended to include the *context* of a subject's interaction with the world, including the social and community context. The community is considered in light of the *culture* of that community. Community norms and division of labor in a community interaction may also come into play. The boundaries of study are not directly limited to the interactions in the user interface itself. Both theories also suggest that speaking and human cognition cannot be separated from action [Kaptelinin et al 2003].

One of the major differences between situated action theory and activity theory is the depth and unit of analysis: situated action theory emphasizes individual actions of persons in a given situation, where activity theory is also interested in durable phenomena that occur across situations over a broader length of time. "In activity theory…an object is (partially) determinative of activity," notes Nardi, "in situated action, every activity is by definition uniquely constituted by the confluence of the particular factors that come together to form one 'situation.'"[Nardi 1996]

From a researcher's point of view, one limitation to both of these models is that they typically require extended ethnographic research in order to determine the situation, or context, in which a particular set of actions is occurring. This can be problematic both for practical reasons and theoretical ones: if a researcher thoroughly analyzes the security interactions of a group of engineers at Boeing, the researcher has no guarantee that those interactions and situations would occur with a set of users who are surfing

the Internet from home. However, the extra work can pay dividends: applying these theoretical frameworks to show the context as well as the specific process of an interaction allows for a level of analysis not possible with the simple usability studies currently common in the field.

Activity theory in the context of this study was used to frame the concept of design work and formulate the research questions and the questions asked of participants. The study did not use activity theory as a lens for analysis but as a starting point for framing the study design. Activity theory also formed an important frame for the analysis of trust relationships, as we will see.

Trust

In 1983, Ken Thompson, longtime pioneer of computer science and one of the architects of the UNIX operating system, won the prestigious Turing Award from the Association for Computing Machinery (ACM). He used the occasion for his Turing Award speech, "Reflections on Trusting Trust," [1984], now itself a classic of the computer security genre.

As an exercise, Thompson wrote a Trojan horse program into a C compiler. The code would reproduce itself into any binary created by the compiler - meaning, he pointed out, that even a program whose every line of code had been written and vetted by trustworthy programmers would still carry the "malicious" payload once it had been compiled using the hacked compiler. "You can't trust code that you did not totally create yourself," Thompson pointed out, though with a modern viewpoint into distributed programming we might rephrase his thought: code cannot be trusted unless every level of the *solution stack* is known to be good. (The solution stack is the set of software components required to create a solution: operating system, networking protocols, middleware, database, applications, etc.)

That said, trust is not simply about trusting code and systems. It is also - indeed, primarily - about trust in people, or trust in institutions. Spinellis [2003] wrote about the problem of a completely trusted system in the days when Microsoft was actively working on a trusted computing platform, in which

every aspect of the stack was known and controllable by the administrator. He regarded the inability to secure the entire stack as a benefit: "Those of us who distrust the centralized control over our data and programs that trusted computing platforms and operating systems may enforce can rest assured that the war for total control over computing devices cannot be won."

Spinellis' point was that the people or institution that control a system cannot necessarily themselves be trusted, even if the system can be fully "known." Nations, corporations, even individuals who control a system may not have the best interests of the system's user at heart.

This tension plays heavily into the question of what "trust" actually is. Defining the term itself has been controversial in the literature, since the definition often carries the viewpoint of a specific epistemology.

One of the early definitions of trust still cited in the human-computer interaction was that of Rotter [1967]: "an expectancy held by an individual or group that the word, promise, verbal or written statement can be relied upon." Rotter was a social psychologist interested in issues of interpersonal trust. More recent work by Nissenbaum [2004], Volken, [2002], and Yamagishi et al. [1999] has led to a more nuanced and information-based definition of trust, involving the concept of truster and trustee, the degree of risk the truster is willing to accept, and the uncertainties the truster may have about the trustee due to lack of information or transparency.

Other writers like Nissenbaum and Cofta [2007] agree that the act of trust is essentially an act of power transfer: you, the truster, are giving a measure of power over you to the trustee, and accepting the risk that the trustee might do something harmful with that power or information. Cofta substitutes the term "control" for the term "power": how much control does each party have and give up in a given communication or relationship? Yamagishi reminds us of the difference between trust, where the truster expects cooperative behavior based on inference of the trustee's intentions, versus *assurance*, based on the knowledge of the incentive structure surrounding the relationship [Yamagishi, Kikuchi and Kosugi 1999].

Put another way, Yamagishi's point is that trust is required in situations where the truster does not have assuring information about the trustee.

All of these theories of trust play into the concept of trust decisions and *trust questions*, an important concept for this dissertation. Interactions with systems often require users to make trust decisions, as we have seen. Do I trust this system or entity with my information? That interaction is based on the principles of trust described here.

Ethics

Another rich field of theoretical study for usable privacy and security researchers is that of *ethics*. For the purpose of this discussion, I will adapt a definition from Floridi [2006]: ethics is the study of "morally qualifiable actions," actions that can cause good or evil, and the decision-making process that leads into making those actions.

Goles et al. [2006] expand on this definition: ethical decisions "are primarily contingent on the perceived characteristics of the issue at stake," and are largely "situation-specific," meaning that the ethical decision is impacted by the different ethical norms inherent in different contexts, such as "work" or "play."

Floridi [Floridi 2006], in a discussion of his proposed framework of "informational ethics," suggests a set of fundamental ethical principles in information systems:

> Entropy ought not to be caused in the infosphere
>
> Entropy ought to be prevented in the infosphere
>
> Entropy ought to be removed from the infosphere
>
> The flourishing of information entities as well as the infosphere ought to be promoted by preserving, cultivating, and enriching their properties.

Floridi [2006] also usefully notes, "there can be moral agency in the absence of moral responsibility. Promoting normative action is perfectly reasonable even when there is no responsibility but only moral accountability and the capacity for moral action."

Discussions of ethics in the context of user-centered security research are multifaceted. Most obviously, security professionals and designers tend to see themselves as having a moral and ethical responsibility to protect the data entrusted to them, or to reduce "entropy in the infosphere" in Floridi's phrasing [2006]. This argument, however, has pitfalls. Consider the ongoing debate of the merits of digital rights management, or DRM. Does the protection of the intellectual property of digital music and video have more moral and ethical force than promoting freedom of distribution and transferability in the open architecture of the Internet? The answer to that ethical question has a direct impact on the business model and designs for music and video user interfaces.

Nissenbaum [2004] writes of the relationship between "trusters" and "trustees," and notes the importance of contextual, mutual and reciprocated trust relationships. Activity theory can be used to analyze these trust relationships. To repeat, activity theory at its most basic level consists of the relationship between the subject, the activity, and the object. Using that analytical model, the user (subject) considers whether to share (activity) the user's data (object) with another entity, *in the context* of the type of data, the user's prior interactions with that entity, and the perceived risk. Implicit in this analysis is the notion of ethical behavior on the part of the trustee: *will the trustee treat my data in an ethical fashion*? Studies of ethics give some insight into the types of behavior that would be perceived as "ethical" or "unethical." This behavior, in turn, affects the trustee's reputation and moral authority, their *ethos*, as described by researchers into rhetoric such as Miller [2004] or Johnson [1998]. Cofta [2007] formalizes the definition of ethical behavior as "trustworthy behavior."

Further, Cofta [2007] analyzes trust in mathematical terms: trust, he says, is an "estimate of the subjective probability of a certain desired course of action in the absence of control." Confidence is the

"subjective probability of expectation that a certain desired event will happen (or an undesired event will not happen), if the course of action is believed to depend on another agent.)

Cofta's [2007] formalized logic analysis allows, in his model, for trust and ethics to be quantified and modeled, within some limits. While confidence can be measured via surveys, games of trust, etc. and assigned a probability, these probability scores do not have a fine degree of accuracy. Users are notoriously poor at self-reporting their behaviors relating to security and privacy. However, Cofta's model [2007] allows for a sophisticated analysis of different implementations of trust management and e-commerce models for their "trustworthiness" or *ethos*.

A core assumption of the usable privacy and security field is that designers should act in an ethical fashion when creating their designs, and that treating the user's data properly is part of that ethical work. This is discussed at length by core works in the usable privacy and security field (e.g. [Cranor and Garfinkle 2005]) and is encoded in the agreements signed by certified information security professionals [Hansche et al. 2004]. If the integrity of the user's data is not preserved or if the data is redistributed in ways not approved by the user, these ethical guidelines are breached.

That said, an interesting question not thoroughly explored in the literature is the level of awareness that designers have about these ethical concerns. This level of awareness will be discussed in forthcoming chapters.

Satisfaction and *Anshin*

Researchers in the field of human-computer interaction have noted that one of the hardest concepts to measure is that of *satisfaction*. [Kaptelinin et al 2003; Lindgaard and Dudek 2003] Satisfaction is one of the fundamental goals of human-computer interaction work, according to the IEEE [Lindgaard and Dudek 2003], but researchers struggle to understand how satisfaction can be evaluated.

For example, does usability equal satisfaction? Older works on usability have implied that usability evaluation can give an estimate of how satisfied the user will be with the interface (e.g. [Nielsen 1993]), but the concept is problematic. Greenberg points out that usability evaluations can give a scientific validation to a user interface model without giving any data about user acceptance or demonstrated need for the model [2008]

Recently, Japanese and American researchers [Murayama et al. 2011; Murayama et al. 2008] have been investigating a Japanese concept known as *anshin*. The word does not translate properly into English. It consists of two kanji characters, "AN" (mind) and "SHIN" (to ease). A very rough translation would be "ease of mind" or "contentment." [Murayama et al. 2008] Its antonym might be "anxiety."

Yamamoto et al. [2011] cite Kikkawa et al. [2003], published in Japanese, as the first to define anshin in terms of technical safety. According to Yamamoto, Kikkawa explained that there were two types of anshin, defined as "ignorant anshin"—which a native English speaker might call "passive anshin," to avoid negative connotations--and "active anshin." In passive anshin, the subject has no direct knowledge of any threat. A subject with "active anshin" is fully aware of the situation and content that their safety and security is protected.

In the context of usable privacy and security, anshin is an intriguing concept. It evolves from trust but is more encompassing. Anshin is the user's overall feeling of security. It is a neat encapsulation of the goal of usable privacy and security—a system that not only provides ease of use and security, but also provides a feeling of contentment in its use.

Trust and ethics form the community norms and framework for the usable privacy and security community. User satisfaction and *anshin* are the goals of the usable privacy and security community. How, then, does the usable privacy and security community conceptualize the activities that involve trust, privacy, and security? In the next section, I will give a brief overview of the usable privacy and security literature.

Usable Privacy and Security Studies

In the next section, I will discuss some of the most well known technical and practical studies in the usable privacy and security field. These studies have set a model that many newer studies in the field follow. The research tradition that they have created has strongly influenced the design of usable privacy and security studies to this day, including mine.

Whitten & Tygar

It is not possible to discuss the usable privacy and security field without discussing two seminal papers within it, mentioned in the first chapter: Whitten & Tygar's "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" [1999] and Adams & Sasse's "Users Are Not The Enemy: Why Users Compromise Security Mechanisms And How To Take Remedial Measures" [1999]. These papers are widely cited within the field as canonical examples of the type of research needed in usable privacy and security. In this section, I will discuss these papers in some detail. Their results are in some ways outdated but their approaches are still in common use today.

Whitten & Tygar were interested in the potential security impact of a usability problem. They wondered if conventional usability standards were sufficient for security concerns. To explore the problem, Whitten & Tygar performed a usability evaluation of PGP 5.0, a then-current open standard for encrypting e-mail. The usability study included both an informal cognitive walkthrough [Beyer and Holtzblatt 1998] and a formal user test. [Nielsen 1993]

PGP 5.0 was an interesting choice of technology to test. Standard e-mail is a very insecure communication technology. Because e-mail is sent across the Internet to the recipient in plaintext, it is vulnerable to a "man-in-the-middle" attack. A malicious hacker can read the contents of the e-mail simply by using a "packet sniffer," a program that reads Internet packets as they go by. As an analogy,

consider a letter written on the *outside* of an envelope that can be read by every postal carrier and anyone standing around the post office.

For years, solutions have been available that allow e-mail to be encrypted in such a way that it cannot be read unless the recipient has the correct "key." One of the most common publicly available solutions was and is the PGP ("Pretty Good Privacy") algorithm, originally developed by Phil Zimmerman in 1991. PGP had been widely available for nearly a decade when Whitten & Tygar performed their study, and yet it was and is rarely used [Gaw et al. 2006]. Perhaps usability problems contributed to the lack of use?

As it turned out, the answer was: yes, absolutely. Only one third of the participants in the user study were able to successfully sign and encrypt an e-mail in a 90-minute session, and of those successful participants, one quarter accidentally revealed the secret they were meant to protect in the process.

This study was a foundational one for several reasons. As the authors themselves noted, it was the first formal usability evaluation performed on a feature that was designed for the sole purpose of protecting a user's digital information. Perhaps more importantly, however, it was the first study to attempt to present formal definitions of "usable security" and the issues that make security unique as a usability problem.

Whitten & Tygar [1999]'s formal definition of "usable security" was as follows:

> Definition: Security software is usable if the people who are expected to use it:
>
> •Are reliably made aware of the security tasks they need to perform
>
> •Are able to figure out how to successfully perform those tasks
>
> •Don't make dangerous errors
> •Are sufficiently comfortable with the interface to continue using it

They also described five usability problems unique to security solutions:

> 1. Unmotivated users. Security is almost never a primary task for a user, but an aspect of another task.

2. Abstraction. Computer security policies are programming abstractions that do not easily fit into a user's mental model.

3. Lack of feedback. Security management is a complex problem, difficult to summarize easily for a user as UI feedback.

4. "Barn doors." Once a secret has been left unprotected, the user must assume that it has been compromised.

5. Weakest link. The security of a networked computer is only as good as its weakest component.

This study went a long way towards defining the parameters of the problem space for usable privacy and security research. It accepted as an assumption that security solutions were necessary for preserving the privacy and integrity of a user's data. It described the issues inherent in the acceptance and use of a security solution by users. The study did not start with the assumption, common in other security studies of the time, that users were not to be trusted with their own security—a point that I will return to in a moment. It noted the inherent paradox of security features: very few users have a primary task of "being more secure today," but if the user's security is compromised during the completion of an unrelated task, that task has failed. It reiterated and paraphrased Saltzer & Schroeder's point [1975]: a security solution is not useful unless it can be used. The study also pointed out the value of using methods traditional to the usability field to explore these issues of psychological acceptability.

Since this study has been published, there have been some refinements in the field. In particular, what Whitten & Tygar [1999] referred to as "security software" has since been slightly redefined: Friedberg [2009] calls it the "trust user experience." This is a subtle but important difference. The "trust user experience" is not just about security, but about trust in a system and in a system provider, a topic I will cover in a few pages.

Then, too, others have noted that traditional usability methods are not the only ways of learning more about this problem space. Recent studies have included approaches such as participatory design [Flechais and Sasse 2009] and user interface pattern recognition [Muñoz-Arteaga et al. 2009] among

others. The field would be limited indeed if there was only one "approved" approach to the problem. However: the approach taken in Whitten & Tygar's paper [1999] was unique at the time and widely imitated since.

Usability

I use the term "usability" in the sense given by Dumas & Redish [1999]:

> Usability means that the *people who use the product* can do so *quickly and easily* to accomplish *their own tasks*. This definition rests on four points: (1) Usability means focusing on users; (2) people use products to be productive; (3) users are busy people trying to accomplish tasks; and (4) users decide when a product is easy to use.

This is an especially useful operational definition for usable privacy and security as it emphasizes the notion of users "trying to accomplish tasks." As a reminder, being secure or private is never the primary task of a user [Egelman et al. 2007]. Usable privacy and security is the art of balancing the usability of the task with the privacy and security requirements and mitigations necessary for that task.

Following in the tradition of Whitten & Tygar, many of the studies in the usable privacy and security field have used traditional usability methods to examine potential issues with user interfaces deemed to have a security or privacy impact. Studies in this area of the field use traditional usability methods [Dumas and Redish 1999; Hughes 1999] to examine usability problems for "trust decisions" and other user interface designs that are deemed to have security or privacy impact.

Lorrie Faith Cranor's CUPS lab at Carnegie Mellon University is especially well known for this type of study. Examples from their work include evaluation of security and privacy indicators in web browsers [Cranor 2005; Egelman, Tsai, Cranor and Acquisti 2009], phishing warnings [Egelman et al. 2008; Zhang et al. 2006], and SSL notifications [Egelman, Cranor and Hong 2008]. Other researchers have looked at the usability of CAPTCHA warnings [Yan and El Ahmad 2008], click-based graphical

passwords [Chiasson et al. 2007], and out-of-band authentication schemes [Al Zomai et al. 2008]. More such studies appear at CHI and other human-computer interaction conferences every year.

While the research community has benefited immeasurably from these thoughtful studies, there are some known limitations to these methods of inquiry. For example, several studies have noted that participants will treat data in a study differently than they would if the data was their own (e.g. [Zurko and Simon 1996]) and often do not accurately self-report security data [Egelman, King, Miller, Ragouzis and Shehan 2007; Sotirakopoulos et al. 2011]. Then, too, there is a more fundamental concern about task analysis. "Being secure" is rarely if ever the primary task of a user:

> Users deal with security infrequently and irregularly, and most do not notice or care about security until it is missing or broken. Security is rarely a primary goal or task of users, making many traditional HCI evaluation techniques difficult or even impossible to use.
>
> Security-related user studies employing observational methods are extremely difficult to design…[as] users only deal with security on rare occasions. [Egelman, King, Miller, Ragouzis and Shehan 2007]

Adams & Sasse

Adams & Sasse [1999] published around the same time as Whitten & Tygar [1999], but took a very different approach to their study. Instead of a usability test of a particular interface, Adams & Sasse opted for using social science methods, a web survey followed by a series of semi-structured interviews on the topic of password use. They then used a grounded theory coding method to analyze the data they had gathered.

The authors noted as their starting point that current information security systems were heavily reliant on user passwords, but that the usability of passwords had not been investigated in depth. In particular, it was not clear whether the then-published security guidelines for password use - change them frequently; use unique passwords for different systems; use difficult-to-guess combinations of

letters, numbers and symbols; never write your password down or keep it in a discoverable place - were followed.

As it turned out, the security guidelines for password use were problematic in real-world scenarios. Users frequently circumvented the password guidelines: using the same password indefinitely, writing them down, re-using passwords in multiple places, or using poorly designed passwords (e.g. "Password" or another easy-to-guess term). The stated reasons for the behavior varied, but Adams & Sasse identified two major themes in the data. First, users frequently had a poor understanding of the security issues and risks that underlay the password requirements, and often proceeded on false assumptions about the nature of the security of their data. Second, users often felt compelled to circumvent requirements in order to get work done.

Adams & Sasse used the data from their study to call for a concentrated research and development effort in applying user-centered design principles to privacy and security issues. "Insecure work practices and low security motivation among users can be caused by security mechanisms and policies that take no account of users' work practices, organizational strategies, and usability," they noted.

The study by Adams & Sasse was foundational in the field in two major ways. First, it established a tradition of looking beyond traditional usability data in examining usable privacy and security. Sasse in particular has noted in conference workshops the importance of working with users in the field to understand privacy and security issues, rather than simply relying on lab studies [Beautement and Sasse 2010]. Second, the "call to arms" for additional work in the usable privacy and security field served as encouragement for many other researchers.

Experience Studies

Following in the tradition of Adams and Sasse [1999], some researchers have eschewed traditional usability testing in favor of investigations of user attitudes, concerns and practices regarding security and

privacy. For example, Friedman et al [2002] looked at the mental models that her research subjects had of data security on the Internet and how people perceived privacy in a public space with and without surveillance [Friedman 2006]. Klasnja et al [2009] found that users had limited knowledge of the security implications of working on an open Wi-Fi network in a public space, such as a coffee shop. Wang et al examined the notion of "regrets" as it applied to online spaces, specifically the online community at Facebook.com. [Wang et al. 2011]

Several researchers have undertaken studies of attitudes towards online privacy, including Tsai et al. [2006], Radics and Gracanin [2011], Nodder [2005], and a long series of studies by Alan Westin (summarized by [Krumaraguru and Cranor 2005]). A common theme in their results is the difference between what users say about their privacy concerns versus their behavior. Often, users who express concern about their privacy online will cheerfully give up that privacy in exchange for a service perceived to be useful, such as public Wi-Fi or location-aware services. This phenomenon is sometimes called the "privacy paradox," and has itself been a subject of recent study [Oetzel and Gonja 2011].

This on-going line of research has been essential in providing data on the attitudes and motivations of users faced with problems of privacy or security. Its methodological weakness is that surveys of attitudes and behaviors are in some ways reactive, reflecting only attitudes as they exist at the time about technologies and assumptions as they currently stand. As noted in the discussion of the social construction of security, this reflection of attitudes in a point in time can be problematic. For example, when Google first introduced its "Gmail" e-mail service, which scanned user e-mails for key words to be used in targeted advertising, privacy advocates were horrified. Today, many web services use keyword scanning of user-generated content, including Facebook, Yahoo, Google Plus and more. [Chopra and White 2007; Nathan and Garnett ; Zheng et al. 2012]. Once considered a breach of privacy norms, today keyword scanning is considered a standard practice.

Information Security

While these papers are not the primary focus of my literature survey, it is important to note the ongoing research on specific, technical security risks and their mitigations. Data security feature studies are one of the oldest lines of research in the usable privacy and security field and typically refer to features that do not directly lead to a user interaction. Examples include studies of potential threats [Carrow 2007; Kayacik and Zincir-Heywood 2008], cryptography analysis [Sharmila Deva Selvi et al. 2008], or the security of the TCP/IP network protocol [Vutukuru et al. 2008].

In general, these studies are more focused on technical issues of security implementation, and less focused on the user experience. However, the line between these studies and usable privacy and security studies can become blurry in instances where security features rely upon user input or user practices [de Carvalho et al. 2008; Jaferian et al. 2011].

Privacy

Some researchers have looked specifically at threats to the data privacy of individual users on a systemic or institutional level. These studies typically look at institutional policies, general design guidelines, or data governance that may have implications for user privacy, rather than specific technical features or analyzed threats.

Alan Westin, a pioneer in the privacy field with his 1967 book *Privacy and Freedom* and 1972 book *Databanks in a Free Society*, for years ran genre-defining surveys of privacy attitudes by consumers and companies in the United States. The survey results are privately held but have been summarized by other researchers [Krumaraguru and Cranor 2005]. One of Westin's key insights, still often used in the privacy literature, is the division of consumers into levels of concern about privacy: "privacy unconcerned," "privacy agnostics," and "privacy fundamentalists." Privacy fundamentalists, Westin found, published

extensively but were often the least represented in consumer surveys. This finding strongly suggests that the conception and importance assigned to privacy issues in the literature may not accurately represent a more general population.

Helen Nissenbaum has published a great deal of work in privacy from a legal perspective [Nissenbaum 1998; Nissenbaum 2004]. danah boyd [2008] has looked at privacy through the lens of how teenagers use the Internet, especially sites like Facebook. Irene Pollach [2007], among others, has reviewed the known problems with privacy policies. Friedman [2005], Iachello et al. [2005], Li et al. [Li et al. 2011], and others have proposed specific models and conceptual ideas for enhancing user privacy.

A key finding of these and other researchers is that privacy concern is both *personal* and *contextual.* A professor may choose to make certain professional information about themselves available through the web or other social media, but may choose to reveal entirely different information to close friends or family. The type of privacy seen as necessary by a college student is not the same as that required by a working professional. This is not to say that college students require any *less* privacy, only that the data seen as a possible risk if exposed may change over time.

Michele Gilman points out that privacy by design can be more than what data you choose to reveal or not to reveal [Gilman 2012]. Consider the welfare recipient, often stigmatized, frequently with more government-mandated intrusions into personal privacy than the wealthy. Instead of mandated home inspections and aggressive interviews, could privacy of the welfare recipients be improved by using technology to evaluate their cases? "Arguably, the more things are automated, the less opportunity there is for insult," Gilman postulates, but she rejects the argument. Developers, she notes, frequently struggle to correctly translate legal codes into rule sets, and are dependent on the accuracy of the underlying (and frequently mis-entered) data. Gilman argues that poor Americans experience privacy differently than persons with greater economic resources because of the on-going and interpersonal interactions they have with government systems.

We can discern some characteristics of information privacy from this work. It involves the confidentiality and integrity of user data but also involves the privacy rights as a whole of the individual. As with other types of user experiences, information privacy is contextual and driven by cultural norms and user needs. Preserving information privacy is not a "feature" that can be written for a system, but rather a mindset and an analysis that must be brought to bear throughout the user experience design process.

Insights

There is a broad and rich research tradition of usable privacy and security studies that take the user as the object of study. There is an equal tradition, borrowing methods like contextual inquiry and textual analysis, of analysis of organizations and systems that may collect, use, or share data and information that identifies or belongs to a particular user.

That said, the user is not the only potential object of study when looking at usable privacy and security design. Designs are not created in a vacuum. They are formed out of the constraints of the design requirements. They draw upon the skills and experience of the designer. They are grounded in the norms of the design community as well as the norms of the larger audience. To understand usable privacy and security interactions, it seemed necessary to understand the activity of *creating* the usable privacy and security interactions.

There is, however, a gap in the research. To date in the usable privacy and security community there has been very little research on the attitudes and practices of the designers of usable privacy and security interfaces. Werlinger et al, among others, have looked at the attitudes and practices of security practitioners [Werlinger, Hawkey, Botta and Beznosov 2009], but I am interested in a different audience. I am interested in the designers whose primary role is *not* security or privacy. The object of this study is the

designers working across a variety of domains who occasionally and intermittently create designs with privacy and trust implications.

It is self-obvious that the majority of designers are not security experts. Nor should they have to be. Security is a specialized sub-field, not core to the work that most designers do day to day. Privacy and trust issues, while important to designers, are also not a universal part of designing user interactions. While there are implicit trust choices in every interaction a user makes, explicit trust decisions to give up personal information are more rare.

In the usable privacy and security literature, we have seen a number of studies that have attempted to give tools or instruction to designers for improving usable privacy and security interactions. However, activity theory would seem to suggest that without a more full understanding of the context, culture, subjects and objects of design for usable privacy and security interactions, these tools or instructions may rely on assumptions about the design process that are not in fact validated by study.

For example, the usable privacy and security literature implicitly states that trust and ethics are strong motivating forces for design. We have seen how core theories on trust, ethics, and user satisfaction are to the framing of usable privacy and security goals and studies. However, it is not clear how much designers are relying upon frameworks of trust and ethics when the designer is faced with a problem of an interaction involving a trust implication.

For these reasons, this study uses the design activity, rather than the user activity, as the primary focus of study. The study is intended to complement the considerable research done on user activity, attitudes and satisfaction in the usable privacy and security literature, by looking at the other polarities in the community: the designer and the process of creating the design. I turn now to a brief discussion of the design literature and methods.

Design and Designers

When I speak of designers, whom do I mean?

I use *designers* in the sense of people who are performing design tasks, as defined by Goel & Pirolli [Goel and Pirolli 1992]: anyone who solves design problems. They define the problem-solving process as having the following structure:

1. Problem structuring
2. Distinct problem-solving phases
3. Reversing direction of transformation function
4. Modularity, decomposability
5. Incremental development
6. Control structure
7. Making an propagating commitments
8. Personalized stopping rules and evaluation functions
9. Predominance of memory retrieval and non-demonstrative inference
10. Constructing and manipulating models
11. Abstraction hierarchies
12. Use of artificial symbol systems

Put more simply, design is a process of problem solving with certain defined stages of development and characteristics. The exact methods and practices of this problem solving depend upon both the genre (software, architecture, etc.) and the task environment (large company, solo practitioner, etc.) Depending on the context, a designer might be responsible for all of these stages or a smaller subset of the larger list.

Design Studies

Norman [1991] and Goel & Pirolli [1992] provide a useful framework for design activity by grounding it as a cognitive problem: designs, says Norman, are cognitive artifacts, "artificial devices designed to maintain, display, or operate upon information in order to serve a representational function." Goel & Pirolli provide a tripartite framework for design research, studying the information-processing system, the design task environment, and the design problem spaces. Both deal with the concept of design as the leveraging and awareness of constraints, a particularly interesting problem in the security realm, which by some practitioners is described as creating a system of properly constructed protocols and constraints [Anderson 2001].

The advantage of this approach is that it allows both the process of design and the artifact created by the design process to be analyzed in some detail. Goel & Pirolli target the process; Norman targets the artifact. A great many studies in the user-centered security literature concentrate mainly on the artifact without thinking about the designer or the process that creates it.

Dorst [2008] points out that design research should not be focused exclusively on the process, but should also be focused on the designer and design activity as a whole. Cross [2004] looks at "expert" designers, and particularly notes that expert designers are "solution-focused" who are pro-active in "problem framing". Dorst, similarly, quotes an earlier study with six levels of designers from "naïve" to "visionary," and notes that experts and visionaries typically "recognize high level patterns in design questions and respond quickly."

Friedman's notion of "value sensitive design" [Friedman 1996] is particularly useful in this space for its notion of examining the values inherent in a particular design issue, and managing the trade-offs between those values. Friedman also makes special note of the concept of direct and indirect

stakeholders, which has large implications for the user-centered security world that will be discussed momentarily.

Beyer and Holtzblatt [1998] in their contextual design work look at the problem of understanding the context in which users are doing their work, and by corollary, the context of the challenges users encounter that designs need to overcome. There are other field work techniques available for learning more about the context of user activities, but the central message of developing design through user data taken not just in the laboratory but in real-world situations is very important in this space.

Norman and Gaver [Gaver 1991; Norman 1988] separately emphasized the importance of "affordances," interfaces that implicitly give information about the properties of a thing to be acted upon. The literature on visuals and indicators in user-centered security situations suggests that affordances may be more problematic in this space. "Passive" security indicators that give information implicitly without requiring direct action from the user typically are not well understood or acted upon by the user. Only "active" indicators have been shown to provide a more secure user experience. Yet the "active" indicators by design are extremely explicit in the information that they give to users. What then would be an "affordance" that would allow for the user to obtain information about how to manage an interaction securely, without interrupting their task flow?

Dorst [2008] as well as Cross [2004], suggest an intriguing problem with the notion of the design guidelines for secure interaction, described in the earlier section. The target audience for guidance on secure interaction design includes not just novice but expert designers, those who have been in the field for years and work on high-visibility products. If such designers are "recognizing high level patterns in design questions," from prior experience, and are largely interested in "framing problems" in ways that they understand and can develop solutions for, does the existing guidance help them to achieve those goals?

Friedman's notion of value-sensitive design, and in particular her ideas of the importance of direct and indirect stakeholders, has considerable force in the user-centered security design space. Take a simple thought experiment: On a university laptop, all other things being equal, would you use an unsecured wireless access point in a coffee shop? Many would say yes. And yet there is risk: communication over such a network is easily intercepted, and an unscrupulous hacker can take over your machine. Perhaps the risk is low enough that you are willing to take the chance; you do not keep anything valuable on your laptop. But what about the passwords that you use to log in to your e-mail over that Wi-Fi network? Access to your e-mail gives the hacker not only your words, but the words of everyone who has written to you as well. Access to a password for a university network account potentially gives access to student grades, research data, and more.

In this case, the direct stakeholder in a trust decision ("do I trust this Wi-Fi network?") is you. But the indirect stakeholders include everyone who has entrusted their information to you, one way or another. In balancing the values of privacy risk vs. the need to get work done, it is possible that more work could be done to show you the needs of the indirect stakeholders as well.

Modularity

In my research, I will focus particularly on one aspect of the design process mentioned by Goel & Pirolli [1992]: modularity and decomposition.

Modularity in design is often referred to in architectural terms. Baldwin & Young [2000] explain modularity in terms of structures:

> A module is a unit whose structural elements are powerfully connected among themselves and relatively weakly connected to elements in other units. Clearly there are degrees of connection, thus there are gradations of modularity.

…and explain the purpose of modularity in terms of design rationalization and simplification:

> A complex system can be managed by dividing it up into smaller pieces and looking at each one separately. When the complexity of one of the elements crosses a certain threshold, that complexity can be isolated by defining a separate abstraction that has a simple interface. The abstraction hides the complexity of the element; the interface indicates how the element interacts with the larger system.

This definition is often used in software design to create building blocks for larger applications. Modularization allows for functional units of code to be created, tested and reused as needed. Once implemented, in conception the coder need not concern herself with the inner workings of the module as long as the module's interface is clear and consistent.

However, trust questions are difficult to reduce to a single module or set of functions. Trust questions are about the relationship between an actor and a system or an actor and an organization, not limited to a single element of an interaction [Clark 2010].

With that in mind, I use modularity in the sense explained by Langlois [2000], who argues that the principles of modularity can be applied to society, organization and transactions as well as systems. In Langlois' view, modularity can be used to "internalize externalities"— meaning, encapsulating complex external effects or requirements in a "module" that is internal to the system. This definition of modularity allows us to consider the complexities of trust in a separate frame, a "module" within the overall design process. In industry, there have been demonstrated efforts in the software industry to modularize concepts of trust through modeling and guidelines [Friedberg 2009; Li, Najafian Razavi and Gillet 2011; Patrick, Briggs and Marsh 2005; Yee 2005].

Decomposition, by contrast, allows for a task or activity to be subdivided into a set of subtasks or functional steps that will resolve the task or activity [Shalloway and Trott 2005]. Decomposition permits the designer to reduce the activity to elements suitable for individual analysis and design.

Summary

My research draws from several of these research traditions but does not fall neatly into any of them. My research questions are primarily influenced by the "experience studies" of security and privacy, and the research into trust and ethics.

Situated action theory and activity theory were important to my thinking about the design and purpose of this study. Both theories emphasize the importance of *context* in interaction, an area not always easy for security experts to engage. Activity theory in particular is useful because of its inclusion of norms of community and mediating objects in the investigation of an activity. Activity theory is often used to interrogate interactions but can be used just as easily to examine the activity of design itself, an important insight for me. For this reason, my study concentrates on the usable privacy and security conceptions of designers.

In the usable privacy and security field this is a novel approach. There have been many studies on specific design solutions. There have been studies on how to influence design thinking. There have been studies that have looked at how IT security managers conceptualize usable privacy and security [Parkin et al. 2010]. However, to date, there has been little investigation of how working designers, not specializing in usable privacy and security, approach problems of trust. In the next chapter, I will discuss the methods I chose to explore designers' conceptions and approach to usable privacy and security.

Chapter 3: Methods

In Chapter Two, I discussed the intersection in research traditions that informs the field of usable privacy and security in general and the investigation of trust in particular. In this chapter, I will explain my research questions and methodology.

Research Questions

The usable privacy and security field in general has focused on the experience and challenges of the user. This is an entirely appropriate if not essential line of study. However, the experiences of the designer who is building that user experience remain relatively unexplored. While there is a considerable literature in design theory and practice, to date there has been little investigation of whether the experiences of designers working on usable privacy and security problems are different in important ways than the experiences of designers working in other areas.

Because this study is exploratory, it cannot make claims about the experience of *all* designers working on usable privacy and security issues. Instead, the goal of this study is a preliminary investigation of how *some* designers have worked on usable privacy and security issues. An additional goal is to suggest future lines of research.

I hypothesize that most experienced designers will consider usable privacy and security issues when they are building an interface that has security implications. However, there is limited data available on the tools that designers use, the assumptions that designers make, and the processes that designers follow when working on interfaces that must help users preserve the privacy of their data.

As a reminder, this study answers the following questions:

First, Fogg [2002] notes that trust questions, which fall under the umbrella of what he calls "persuasive technology," work best when the problem space is narrowly defined and the audience is already receptive. For the designers studied, how do they define their problem space and their audience?

Second, to use the terminology and theoretical framework of Goel & Pirolli [1992]: how do designers structure their approach to design problems of usable privacy and security? How do they create modularity and decomposability of these problems?

Third, how do designers conceptualize the problem of trust questions in relation to the overall design space in which they are engaged? In what contextual relationship and framing do they place trust questions?

To address these questions, I performed an open-ended study using survey and interview data to investigate (in Dorst's words) the actor, the context, and the structure and dynamics of the design approach to trust questions. For the following approach, I am indebted to the framing of Goel & Pirolli [1992], Dorst [2008], and Zimmerman et al. [2007] as well as discussions with Cynthia Putnam [2010].

To use the terminology of Teddlie & Tashakkori [2003], I chose to use mixed methods for both strength of inferences and diversity of views. Taken individually, both the survey and the interview methods had potential weaknesses. The survey could reach a broader sample of designers, but did not allow for any probing or follow-up questions regarding their decisions or approach. The interviews could not reach as broad a variety of designers. Taken together, however, the methods provided both breadth of sample and depth of information. Each provided complementary strengths of analysis. [Lieberman 2005] The survey, primarily quantitative, was performed first and informed the qualitative interviews.

Object of Study

User experience (UX) designers are the objects of my study. However, the definition of "design" varies widely depending on the writer. How can we best define "designers" for the purpose of this study?

To reiterate, my concept of the designer was borrowed from Goel & Pirolli [1992]. Anyone who solves design problems, using certain defined stages of development and characteristics, qualifies as a designer for the purposes of this study. The exact methods and practices of this problem solving depend upon both the genre (software, architecture, etc.) and the task environment (large company, solo practitioner, etc.) Depending on the context, a designer might be responsible for all of these stages or a smaller subset of the larger list.

Survey

The first stage of the study was a survey of designers.

In reviewing the research questions at hand, two immediate methodological problems presented themselves. The first was the common problem of population sampling. The study sought input from many different designers performing a variety of meta-activities across several design contexts. It was hoped that this would help to highlight any hidden assumptions that were made by practitioners in a specific design context.

The Seattle area, where I lived at the time the study was conducted, is known for its high tech industry. It would be possible to pick certain organizations of varying size and contexts and recruit specifically within those organizations. However, there was a potential sampling bias in that method that I wanted to avoid. Many of the designers in the area, even those working in smaller or non-profit organizations, have experience working with one or more of the three major high-tech employers in the

area: Microsoft, Boeing, and Amazon. Each employer has a strong tradition of design with its own guidelines and professional mores. While I had no problem with including these designers in my population, I wanted to avoid limiting the sample to people with experience in one of those three organizations.

A snowball sample seemed a reasonable compromise. Snowball sampling is a form of chain referral sampling, in which the initial pool of participants is asked to recommend additional participants eligible for the survey, increasing the pool with each new round of additions [Biernacki and Waldorf 1981]. Snowball sampling was originally popularized for use with at-risk or hidden populations, but can also be used for any population with strong connections between participants [Biernacki and Waldorf 1981].

One known characteristic of the design profession is that its extensive use of feedback and shared goals leads towards strong professional connections between experienced designers [Cross 2004]. Snowball sampling using these connections provided a systematic way of finding highly experienced designers from a variety of different venues.

The major known weakness of snowball sampling is the difficulty in capturing a representative subset of the population. By its nature, snowball sampling tends to oversample from the specific groups where the initial "seed" sample was created. To help mitigate this problem, it was judged that an Internet-based survey would avoid the pitfall of oversampling from people in a specific geographic region or business group. The snowball sample, if properly seeded, would allow for people from many backgrounds and regions to participate.

To create the original sample, the original survey request [see appendix] was sent to Internet-based professional mailing lists and groups on the LinkedIn professional social networking site. It was also sent to specific contacts with extensive resumes of speaking engagements and thought leadership work in the fields of usability and user experience design. These contacts were selected with an eye towards finding different sub-fields and backgrounds in design. To my knowledge, none of the specific contacts that were

part of the initial sample were familiar with each other. Each contact forwarded the recruitment e-mail using both public notices such as Twitter and private forums at their organizations.

To achieve further diversity in the snowball sample, one of the questions in the survey itself also included a request for commonly used Internet forums or other professional networking opportunities. I will discuss the results of this question in Chapter 4, but it is worth noting here that I also used the answers to this survey question to find additional contacts for a recruitment e-mail. This process was repeated for 3 rounds as new forums and contact information were added to the survey data pool.

The survey, called the "Design and Development Survey," was administered in October and November, 2010. The survey was conducted exclusively online.

To further mitigate the problem of oversampling particular populations, the survey included several demographic questions designed to look at whether . These demographic questions were analyzed against a null hypothesis to determine if the sample was a skewed representation of the potential population. The analysis of these questions will be discussed at length in the results section.

The recruitment e-mail was designed to appeal to a broad base of designers, not just those who had encountered a trust problem. The survey call and snowball sample strategy were both designed to attract experienced and expert designers over those in school or new to the profession.

Returning to the research questions, the survey was designed not as an end in itself but to provide background for the study as a whole. The survey was intended to:

1. Develop as broad a sample as possible of the target population

2. Establish the sample of actors (designers, communities of practice) who are working on user interfaces involving trust questions

3. Establish the context(s) in which the sample participants worked

4. Determine whether designers in the sample were statistically likely to have encountered a problem relating to a trust question, as defined in this study

5. Obtain broad information about the approach taken by the participants towards addressing trust problems

The survey was designed to elicit examples of these actors, issues and questions that could illuminate further discussion and research direction. An additional purpose of the survey, as noted, was to identify and recruit designers who would be willing to participate in future stages of the study. As an exploratory study, the survey did not use formal hypotheses in its design.

Finally, the survey allowed for the identification of some examples of "wicked" problems in designing trust decisions and other user experiences for usable privacy and security. I use the term "wicked problem" in the sense of a problem difficult to solve because of contradictory requirements or complex interdependencies. Many usable privacy and security problems fall into this category.

In general, the survey was designed to ask three categories of questions.

Demographic questions. In the case of this survey, the questions were intended to cover both basic demographic questions such as gender and "professional" demographic questions such as length of time in the field.

Experiential questions. One of the primary research questions of this study was to look at how often designers were faced with problems of usable privacy and security. The survey asked several questions intended to discern if the designer had prior experience with the type of usable privacy and security problem covered by the study.

Resource questions. In the case of designers who had experience with usable privacy and security problems, what resources had they used to resolve these problems?

The order of categories and questions was influenced by consideration of order effects. Leading with demographic questions would provide the maximum visibility into the viability of the sample even if participants elected not to complete all the questions on the survey. Experiential and resource questions were arranged in two parts: one for a general audience of designers, one for designers who had worked on usable privacy and security problems.

As translation resources were not available, the snowball sample request and survey were written in English. A follow-up study with multi-lingual participation would be of great value.

Participants were not asked for any personally identifiable information save those who volunteered to be contacted for a follow-up interview. For interview candidates, an e-mail address was requested.

The survey was hosted on the University of Washington's Catalyst Tools web site. Participants could skip questions or return to previous questions. The survey ran from August 19, 2010 to November 29, 2010.

The survey included several questions asking for details about the participant's professional experience. These free-writing questions included the following disclaimer:

> Please do not include any information covered under a non-disclosure agreement (NDA).

Data from the survey was analyzed using SPSS PASW Statistics 18.0.3 for Macintosh and Microsoft Excel 2011 for Macintosh.

In the following sections, I will describe the survey methodology and questions in detail.

Demographic Questions

To understand the reliability of the results, we must understand whether the participants involved with this study provided a balanced sample of a broad spectrum of backgrounds in design. To help answer this question, the survey asked several demographic questions of the respondents. This may seem an intuitive step for the study, but in fact was chosen with some care.

To be clear, it was explicitly *not* an objective of the study to interrogate any questions about the demographics of the design profession as a whole. A snowball sample of a very large population is not enough data to allow for conclusions to be drawn about the demographics of that population as a whole.

Instead, the demographic questions in the survey were designed to evaluate the quality of the snowball sample. As noted earlier, one of the pitfalls of the snowball sample technique is the potential for a non-representative sample based on poor seeding or on deriving your participants from a sample that uses a social network too closely related. As part of the design of this study, the snowball sample used several different Internet forums and unrelated networking contacts to try to counteract this potential bias.

The objective of the demographics questions in the survey was, put simply, to answer the following question: How well did the mitigations work? Did the sample provide a broad variety of participants?

The demographics questions were divided into five categories:

1. Role.
2. Organization size.
3. Time in profession.
4. Gender.
5. Age.

Note that despite the geographic location being a potential concern, the survey did not ask participants to reveal their geographic location. This was a deliberate choice, designed to help preserve the anonymity and privacy of the participants. In retrospect it might have been possible to construct a question that would provide some geographic clarity without intruding on the privacy of the participants, e.g. “Please identify the city you live in or the major city closest to you.” At the time the survey was created, however, it was judged that any geography question would either be too broad

("Please enter your country.") or a potential request for personally identifiable information ("Please give your address.")

Role & Employer

The first question of the survey asked participants to identify their "professional title," and clarified the question: "What title would be listed on your business card?" Participants were given a short free-text field to enter their answer.

The goal of this question was to look at the participant's role within their organization. The use of a "professional title" to determine a role is not a perfect measure by any means. A role of 'user experience architect" may have different responsibilities, level of authority, job skills and experience depending on the organization and on the background of the person filling the role. That said, the use of the professional title had a few known advantages. In the corporate world, to the extent possible, human resources directors strive for consistency in job titles in order to make recruiting and hiring easier. A professional title is a concise, relatively consistent way of explaining the job role to others. Consider the use of the job title on a business card, where the job title is meant to give an indication of the responsibilities and skills of the individual named on the card.

The second and third questions were designed to gauge the experience level of participants. Question 2 asked the participant "How long have you been working in *your current position*?" Question 3 asked "How long have you been working in *your profession*?" (emphasis added in both cases) Both questions used a 5 point scale with the values "Less than 6 months," "6 months - less than 1 year," "1 year - less than 5 years," "5 years - less than 10 years," and "10 years or more."

The questions were designed to illuminate two points. The first was the experience in a *single job role*, while the second was the experience *over the course of a career*.

The fourth question was an optional short answer question that asked participants to list their "favorite professional e-mail lists, forums, or other online networking locations." The answers to this question were used to aid the snowball sample.

Were participants involved with large organizations, small organizations, or solo practitioners? The design literature suggests that an expert's approach to design is similar regardless of the size of organization, but for the purposes of this study it was judged useful to inquire more deeply. As will be seen, one of the questions of the study was about the resources used by the designer. Some resources only made sense in the context of organizations, such as a "mentor or supervisor" or "a co-worker."

The survey asked two questions about the relative size of the participant's employer. Question 5 was a simple yes/no question: "Are you a consultant / self employed?" If the participant answered "Yes," they moved on to the next section. If the participant answered "No," they were asked Question 6: "What is the approximate size of your current employer?" This was a multiple-choice question that asked the user to select from one of the following possible responses:

1. Less than 100 employees
2. 100 − 500 employees
3. 501 − 2000 employees
4. 2001 − 10,000 employees
5. Over 10,000 employees

The ranges for values 1, 2 and 3 were selected as common definitions for "small business" from the US Small Business Administration [2010]. Value 5 was selected as an industry standard range for "enterprise" level business. The remaining value 4 was designed to cover the intermediate range between small and enterprise level businesses.

Age & Gender

Question 7 asked the participant to rank their age on a 5 point scale: "18-24," "25-34," "35-44," "45-54," "Over 55." Question 8 asked the participant their gender. Both questions were optional.

"Question 9" asked participants to enter a code they were given with the survey. This was a procedural question. Some of the participants had requested a code by which respondents from certain forums could be identified. The codes were not used consistently and the answers to this question were discarded from the data.

Experiential Results

Designers often work in a variety of contexts on a range of design types, as noted in the design literature. To use the language of activity theory, it was important to understand more about both the objects that the designers were creating and the context in which those activities were performed. With this in mind, the survey asked designers to describe the type of audience that they most often designed for, and the type of user experience design they most often created. These questions were probed more deeply in the design interviews, described later.

Audience & Analysis Questions

The participants in the survey were self-identified as designers, but "designer" is a broad term. What context did the designer work in: Industry, academic, or a mix? Were they most familiar with designing web sites or mobile user interfaces or something else? It was important to clarify the types of experiences of the designers in our sample.

Question 10 asked "What audience(s) do you typically create designs for?" The question asked participants to pick from the following list. The participant could pick as many of these categories as applied:

1. Individuals
2. Non-profit organizations
3. Academic institutions
4. Government organizations
5. Small-to-medium businesses (less than 500 employees)
6. Large and enterprise level businesses (500 employees or more)
7. Other: please specify.

This question, by design, combined two concepts. The primary concept could be referred to as the *genre* of the audience. Some designs are primarily intended for what marketers often call the "consumer" space, such as a game, or a web site intended for personal use. Some are intended for use in a specific class of organization, such as government or non-profit or business. Some combine several or all of these categories - for example, a word processor, or an instant messaging client. And some designs, of course, do not fit neatly into any of these categories.

The second concept related specifically to the notion of a business market. Designs intended for business use are often tailored to a particular size of organization. For example, a calendaring solution for a small business has a very different feature set and construction than a calendar solution for a large enterprise. The question therefore divided the notion of "small to medium" business and "large and enterprise level" business. The dividing number was set at 500 employees, a common reference number used in American tech industry market segmentation.

It was expected that many of the designers would work across a range of audiences, and this proved to be the case.

Similarly, Question 11 asked "What type of designs do you usually create?" The question asked participants to pick from the following list. The participant could pick as many of these categories as applied:

1. Web sites
2. Software interfaces
3. Mobile device interfaces
4. Hardware interfaces
5. Games
6. Servers or databases
7. Non-technical interfaces (e.g. maps & signage)
8. Other

The first five categories were derived from a set of domains of use. Any device with a browser could use web sites, while software interfaces were typically limited to computers and laptops. "Mobile device interfaces" was a category designed to separate out scenarios for mobile phones, tablets or other mobile devices from the first two categories. "Hardware interfaces" were conceived as those that involved ergonomic design of input devices such as a keyboard. Game design is often categorized as a specific sub-specialty of design [Kim et al. 2008].

"Servers or databases" are not, in themselves, user interfaces. However, user interfaces often relate to and are directly correlated with a server or database. I was interested to learn what percentage of the self-identified user interface designers would also self-identify as working on server or database design.

"Non-technical interfaces" was a carefully chosen catchall term to indicate user interfaces that were not based on digital products, like mobile devices, or hardware interfaces, like a physical input device (e.g. mouse) or a machine like a car. The common example of a non-technical interface, mentioned in the question, is a wayfinding tool such as a map or signage, or product packaging.

Trust Questions

One of the key questions of the study was a simple one. The usable privacy and security literature treats trust questions as a primary, common issue in user experience design. Based on the experience of real-world designers, could the data provide any support for that statement?

Question 12 was a simple yes/no question:

Have you ever worked on a design that gathered or stored personal information (e.g. credit card information, address, financial or health information) from individuals?

Put in terms more common to the world of privacy, the question examined whether designers had worked on a design that collected personally identifiable information, or PII. It specifically called out personal health information, or PHI, and financial information as examples. PHI and financial information — also known as "sensitive PII" — are two areas of special concern for privacy advocates.

The exception in the example list was the address. Contact information such as an address is only considered personally identifiable information if the address is linked uniquely to a user by a name or unique identifier. This subtlety was not explicitly explained in the question to avoid confusing participants not as familiar with the details of privacy regulation. To give some guidance towards what the survey was looking for, the question asked for examples of designs requesting "personal

information" such as "address" "from individuals." The address was included as an example of a piece of PII that is not considered "sensitive PII" under normal circumstances.

For those participants who answered "No" to this question, the survey skipped ahead to a question about forums for professional networking, described later in the chapter. Those participants who answered "Yes" were asked for additional details about their experiences with creating designs involving trust questions.

Details of Design Problem

For those survey respondents who noted that they had worked on a design problem involving a trust question, the survey asked the participant to reflect on an example of the design problem they had experienced. The specific instructions were as follows:

For the questions that follow, please think of **ONE (1) project** that you have worked on **that required you to gather or store user information**. The more challenging the project, the better.

Question 13 asked the participants to select the type of design project they had in mind. The categories offered were the same as in question 11:

1. Web sites
2. Software interfaces
3. Mobile device interfaces
4. Hardware interfaces
5. Games
6. Servers or databases

7. Non-technical interfaces (e.g. maps & signage)

8. Other

Participants could choose as many categories as they wished.

Question 14 asked the participants the intended audience for the design project. The categories offered were similar to those used in Question 10:

1. Individuals

2. Non-profit organizations

3. Academic institutions

4. Small-to-medium businesses

5. Enterprise level businesses

6. Other: please specify.

Unlike Question 10, Question 14 did not include the concept of a "government" audience. This eliminated any confusion between "government" and "enterprise level business," which often have similar design needs. Questions of designing for private versus public sector audiences are outside the scope of my current work.

Question 15 asked the participants about the types of user information the design collected or stored. To define the types of information according to potential privacy impact, the types of information given were those given in an early rendition of the Microsoft Privacy Standard for Development [2010]. They were:

1. Anonymous or pseudonymous information (e.g. User IDs not tied to a real name, aggregated usage data)

2. Real name

3. Phone number, address, or unique government identifier (e.g. social security number)

4. User-created public content (e.g. status updates, public forum posts)

5. User-created private content (e.g. documents not available publicly)

6. User contact list ("buddy list" or address books)

7. Credit card number

8. Other financial information (e.g. bank accounts, financial plans)

9. Other: Please specify. Please do not include any information covered under a non-disclosure agreement.

Question 16 asked participants: "In your professional opinion, how simple was this design problem?" Answers were given on a 5-point Likert scale ranging from "Very simple" to "Very complex."

Question 17 was a long response question. The survey asked participants to explain any "specific challenges to the design problem." This wording of this survey question was deliberately designed to allow the participants to select any aspect of the design problem that they wished, not just those aspects relating directly to usable privacy and security.

The question of "specific challenges" was the only qualitative question on the survey and requires a different type of analysis based on themes in responses. Answers were typically succinct, ranging from a sentence fragment to a few paragraphs. For this question, the data was coded using a thematic approach rooted in constructivist grounded theory, with reference to the usable privacy and security literature referred to in chapter 2. I will explain the qualitative analysis in more detail shortly.

Question 18 asked participants to select the resources they used to resolve the problem from an available list. The list was drawn from an analysis of commonly available tools and resources consulted by designers during the design process, with reference to Cross' theories on how designers gain knowledge [Cross 2001].

Questions 19 and 20 were procedural questions that asked participants if they were willing to participate in the follow-up study.

Design Study

The second stage of the study used a semi-structured interview format to probe the problem space of the designer, as well as the structured approach, modularity and decomposability of their design problems. While the survey provided some insights into a broad variety of professional designers, the depth of information that could be recorded was necessarily shallower, and it was not possible to ask follow-up questions.

The interview subjects were a subset of the survey respondents. Each interview subject had already participated in the survey before being recruited for the interviews. The subjects were chosen as follows:

The snowball sample recruiting for the survey yielded a total of 144 respondents [Dillman 2011]. Of those respondents, 96 indicated that they were eligible for the interviews by noting that they had encountered a trust question. (See chapter 4 for a full explanation.) 31 of those respondents indicated that they would be willing to participate in an interview.

The six participants in the interviews were chosen based on their responses to the survey: each of them posted a thoughtful response about a trust question in a different domain of design work. I will go into detail about the background of the interview respondents in Chapter 5.

All of the interview subjects were designers of web sites, mobile device user interfaces, and/or desktop software interfaces. This is a subset of the overall sample of designers. Future studies might

pursue other types of designers, such as those of multi-modal interfaces like the controls of a car or an airplane.

The interviews were semi-structured in nature. The design of the interview was taken from work by Charmaz & Belgrave [2003]. It loosely borrowed from the "critical decision method" of knowledge elicitation described by Klein [Klein et al. 1989] and later refined by Hoffman [Hoffman et al. 1998, Hoffman and Lintern 2006].

As noted, the pool of interview participants was drawn from the respondents to the survey. Each of the participants agreed separately to the interview, and verbally gave consent.

Designing the semi-structured interview posed some methodological problems apart from those already mentioned in the methods chapter. The primary concern was not introducing bias into the study by 'leading' the participants into answers about security and privacy.

The literature describes two consistent methodological problems in usable privacy and security studies. First, usable privacy and security studies tend to suffer from a form of expectancy bias, where the researcher's interest in usable privacy and security tends to influence the results. Participants often do not accurately self-report data about how they work with security issues, tending to report that they treat security concerns with more care than they actually do [Egelman, King, Miller, Ragouzis and Shehan 2007; Sotirakopoulos, Hawkey and Beznosov 2011].

Second, "being secure" is rarely if ever a primary task of a user. Designers necessarily have to take security into account, but how much attention do they pay to security and privacy issues? This was a key question of interest in the study. Given a sample of designers who do not self-identify as security experts or primarily interested in security issues, and given that security is not a primary task, how would designers reference thinking about privacy and security in their reflections on their design process?

A key methodological concern of the semi-structured interviews, then, was ensuring that the interviewer did not "push" the subject of usable privacy and security. It was important to talk about the

design process in general terms, and introduce usable privacy and security issues only as an additional topic near the end of the interview. This would allow the space for designers to reveal their thoughts about usable privacy and security design without, for the most part, being "prompted" by the interviewer or by the pre-defined interview questions. These questions were:

How did the project get started?

Tell me about the team that helped create this design. Who was involved?

At what point in the process were you brought in to help?

How many design iterations did you go through?

Did the team do any user research? Tell me about it.

What other resources did you use when you were thinking about the design?

What did the first iteration look like?

What changed between that and the final iteration?

How did you decide on those changes?

At the same time, it was important not to ignore usable privacy and security issues entirely, lest the study become moot. To that end, in the interview protocol, two questions were asked *after* the questions about design process:

You mentioned in the survey that the project collected [[these kinds]] of user information. Can you say more about the information that was collected?

Could you tell me about any concerns that you or the team experienced regarding collecting that information? What were they?

The full interview protocol is reproduced in Appendix C.

At its core, the question of a designer's approach to a usable privacy and security problem can be divided into two concepts: a knowledge elicitation and a cognitive task analysis. Knowledge elicitation is learning what the expert knows about a particular problem. Cognitive task analysis, a term of art from applied psychology, asks the following question: Faced with certain inputs and a complex task to perform, what can we say about the mental model and process that the expert goes through to resolve the task?

Multiple researchers have raised methodological concerns about the reliability, validity and reproducibility of cognitive task analysis methods (c.f. Hoffman et al for a full discussion). It was and is considered difficult to achieve agreement on a set of criteria for assessing the cognitive task analysis methods, given that the methods invariably differed widely in procedures, tasks, analysis methods and applications.

The critical decision method is an evolving, validated method for collecting naturalistic data about a task in order to perform that task analysis. It asks experts - designers, in this case - to recall the decisions they made in a specific, memorable "non-routine" event.

The interviews used the concept of the specific, memorable event as a starting point. The interview subject was asked to recall a "wicked problem" in designing a trust decision or other trust user experience from their previous work. Each subject's chosen experience then served as the focal point for the interviews, rather than asking the participants to reflect on their design process in general. This scope grounded the discussion and allowed for attitudes, approach and concerns to be discerned and analyzed.

In the end, the projects described did not lend themselves to a full use of the critical decision method analysis. Two concerns emerged. First, the designers had varying degrees of involvement with the process and constraints under which they were working. The scope of the decisions that were available to the designers varied widely. Second, the projects described had been far enough in the past by the time in

the interviews that they were no longer "fresh" in mind. Several of the participants were not able to state with precision the order in which decisions occurred, or the specific rationales behind a decision. Instead, the analysis of the interviews used a grounded theory approach [Glaser and Strauss 1967, Sullivan 2009, Birks and Mills 2011].

Grounded theory provides insights generated directly from the data. Rather than developing a hypothesis before data collection and then testing it against the data, grounded theory allows for the hypotheses and theoretical framework to emerge from the qualitative data collected during the interview process. This approach is ideal for an exploratory study, where the data must be approached without pre-conceptions. Grounded theory allows for connections to be drawn from different concepts that have emerged directly from the transcripts.

In the case of this study, I used a constructivist grounded theory analysis [Mills et al. 2006, Charmaz and Belgrave 2003]. Constructivist grounded theory suggests that researchers must search for and question implicit meanings of value, belief and ideology in the data, through active participation in the interview and immersion in the narrative of the participants. It requires that the participant's voice and meaning be given prominent place in the final theoretical outcomes, and suggests a style that includes evocation as much as analysis.

I performed a coding process twice at an interval of approximately one year. The first coding process was limited to thematic analysis and open coding. The second analysis was performed according to the staged categorization approach suggested by Burnard [1991].

This was an especially useful approach for interrogating issues of trust and privacy in the data set. Usable privacy and security issues were embedded in the participants' feedback in ways that were not always literal or direct. A constructivist grounded theory analysis allows for those issues to be illuminated and scrutinized at greater length.

The interviews were recorded using a digital audio recorder supplemented by handwritten notes by the interviewer. The interview recordings were professionally transcribed and the transcriptions are reproduced in Appendix D. Coding was recorded using TAMS Analyzer. Interviews were conducted between January 1, 2011 and March 31, 2011.

In the next chapters, I will discuss the results of the survey and interviews described here.

Chapter 4: Survey Results

As noted earlier, the Design and Development Survey was targeted at designers. It was designed to ask three categories of questions:

Demographic questions.

Experiential questions.

Resource questions.

Experiential Results

To review, one of the research questions for the overall dissertation was to look at how the participants defined their audience and their problem space. The following questions were intended to answer these questions. The survey asked designers to describe the type of audience that they most often designed for, and the type of user experience design they most often created.

Audiences & Designs

The first audience-related question was a multiple choice question: "What audience(s) do you typically create designs for? Please select all that apply."

The responses (n=143) were as follows:

Table 1: Typical audiences for designers.

Answer	Frequency	Percentage
Individuals	48	33.6%
Non-profit organizations	40	28.0%
Academic institutions	51	35.7%

Government organizations	29	20.3%
Small to medium businesses (less than 500 employees)	68	47.6%
Large and enterprise-level businesses (500 or more employees)	77	53.9%
Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).	7	4.9%

Many respondents selected multiple categories:

Table 2: Number of audience categories selected by designers

# of categories	1	2	3	4	5	6
# of respondents	62	31	20	21	3	6

The results suggested that the sample of designers favored those who created designs for business. 101 out of 143 respondents (70.6%) identified themselves as designing for small to medium businesses, large and enterprise-level businesses, or both. Note, however, that of those 101 respondents, 59 (58.4%) designed for other audience categories as well.

Except for the "Other" category, all of the audience categories were noted by at least 20% of the respondents. This suggested that the participants in the sample were indeed familiar with a broad range of audiences and audience analysis.

The responses in the "Other" category all indicated that the interfaces created were "in house" or an "internal application" - meaning, essentially, the audience was the institution or employer where they worked. One unique example was the respondent who noted that their audience was "Skilled Trades" at an academic institution.

The next question asked participants, "What type of designs do you typically create? Please select all that apply." The results were as follows (n=143):

Table 3: Typical design types created by designers

Answer	Frequency	Percentage
Web sites	116	81.1%
Software interfaces	81	56.6%
Mobile device interfaces	38	26.6%
Hardware interfaces	9	6.3%
Games	5	3.5%
Servers or databases	20	14.0%
Non-technical interfaces (e.g., maps & signage)	18	12.6%
Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).	20	14.0%

A large majority of participants (81.1%) indicated that they worked on web sites, with software interfaces second at 56.6%.

Twenty respondents selected "Other" and added further information. Five mentioned that they worked on paper products such as documentation and marketing. Four noted that they worked on design and display in retail environments. One respondent worked on "automotive" products, while another worked on "voice user interfaces (VUI)."

The results indicated that while there was a large sample of web site designers among the participants, designers who typically worked in other genres were represented as well.

Trust Questions

The key question of the survey was a yes / no question: "Have you ever worked on a design that gathered or stored personal information (e.g. credit card information, address, financial or health information) from individuals?"

The results of the question were (n=146):

Table 4: Number of designers who worked on a trust question

Answer	Frequency	Percentage
Yes	96	65.7%
No	50	34.3%

A substantial majority of the designers in the sample had, in fact, created one or more designs that had gathered or stored personal information. In other words, their designs included a request that required the user to decide whether to trust the system and organization—i.e., a trust question.

While it was expected that a number of the participants would have experience in usable privacy and security problems, the high percentage was a surprise. It suggested that usable privacy and security problems are indeed a common area of concern for working designers who do not specialize in privacy and security problems.

There were no significant correlations between the response to this question and the designers' level of experience, or the size of the organization they worked in, or the type of audience for which they typically created designs.

Details of Design Problem

Participants who had noted they had worked on a design problem involving a trust question were asked to think of a single, memorable design problem that involved storing user information. They were then asked to identify the type of design project, using a single answer only. The results were (n=96):

Table 5: Type of design project identified by designers

Answer	Frequency	Percentage
Web site	67	69.8%
Software interface	16	16.7%
Mobile device interface	1	1.0%
Hardware interface	1	1.0%
Game	0	0.0%
Server or database	2	2.1%
Non-technical interface (e.g. maps & signage)	0	0.0%
Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).	9	9.4%

Of the "Other" answers, 3 participants indicated that they were working on a "web application." One participant specified that they worked on a "web enabled connected service" with related desktop, mobile and web user interfaces. One noted that they worked on a "web site plus database back-end." Two participants noted that they worked on voice user interfaces. One indicated that they worked on a "catalog." One gave no details.

The overwhelming majority of participants who encountered issues involving personal information, therefore, worked on a web site or software user interface. This finding made some common sense—maps, signage, and hardware rarely require the user to enter any type of personal information.

Next, participants were asked to select the intended audience from an available list. Participants were allowed to select multiple answers or write in their own. The results were (n=96):

Table 6: Intended audience for design project

Answer	Frequency	Percentage
Individuals	57	59.4%
Non-profit organizations	11	11.5%

Academic institutions	10	10.4%
Small to medium businesses	29	30.2%
Enterprise-level businesses	28	29.2%
Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).	7	7.3%

A majority (59.9%) of participants noted that their audience was "individuals." A nearly equal majority (59.4%) indicated that their audience was a small-to-medium or enterprise-level business. These findings appear contradictory on the surface but in fact are resonant: a design for a business may be intended for use by individuals at the business (e.g. an internal issue tracking tool) or by the business as a whole (e.g. a server-based financial system). Designs intended specifically for non-profits and academic institutions were represented as well.

The "Other" section invited short responses. Three respondents indicated their audience was "government" or "federal agencies." Two respondents noted "hospitals" or "public health sites." One indicated the audience was "prospective students." The remaining respondent who selected "Other" did not enter any specific information.

Participants were then asked to select the types of user information that the design collected or stored. The results were (n=96):

Table 7: Types of information collected

Answer	Frequency	Percentage
Anonymous or pseudonymous information (e.g. user IDs not tied to a real name, aggregated usage data)	29	30.2%
Real name	76	79.2%
Phone number, address, or unique government identifier (e.g. social security	78	81.3%

number)		
User-created public content (e.g. status updates, public forum posts)	19	19.8%
User-created private content (e.g. documents not available publicly)	28	29.2%
User contact list ("buddy list" or address books)	10	10.4%
Credit card number	43	44.8%
Other financial information (e.g. bank accounts, financial plans)	27	28.1%
Medical information	16	16.7%
Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).	12	12.5%

Respondents indicated a variety of types of user information, but the two most common types listed were real name (79.2%) and unique identifier (81.3%). This makes intuitive sense as the link of data to a real name or unique identifier is what separates "personal information" from other kinds of information collected. Credit card numbers were also a commonly collected item (44.8%), indicating that a common scenario for these designs may have been an online financial transaction.

To evaluate the complexity of the overall design problem, the survey asked the user to rate their design problem's complexity on a five-point Likert scale, based on their own experience. The results were (n=96):

Table 8: Problem complexity self-rating

Answer	Frequency	Percentage
Very simple	4	4.2%
Simple	9	9.4%
Neither simple nor complex	38	39.6%

Complex	39	40.6%
Very complex	6	6.3%

Most of the design challenges were rated as "neither simple or complex" or "complex" (80.2%).

The evaluation of the design problem's complexity in the data was not significantly related to the experience level of the designer.

Design Challenges

The survey asked participants to explain any "specific challenges to the design problem." As noted, this was an long-form response question, coded and evaluated through a thematic analysis. 58 participants responded to this query.

The identified challenges included technical problems, stakeholder concerns & business strategy, and concerns about user emotion & trust. Intriguingly, a complex issue of identity was also raised. I will discuss these issues below.

Technical Challenges

Predictably, fourteen of the participants cited specific technical challenges or constraints as being their primary concerns. These ranged from hardware limitations ("small screen size of mobile devices") to performance issues ("the processing time was exceedingly slow") to system interfaces ("associating information…such that changes in one area automatically propagated to another area") to restrictions on available UI designs ("the platform was outdated and it ruled out many good UI practices").

Twelve of the participants also cited the common user experience problem of conveying information succinctly. It was not apparent from the data set whether these responses referred to conveying

information regarding user privacy, or conveying information more generally. Contextual analysis of the responses suggests the latter. Obtaining informed consent for use of user information was one of a series of information problems that faced the designers.

This reinforced the idea that, among the set of participants, usable privacy and security problems were one of a variety of design issues that faced them in their daily work. It was also suggestive: while the overarching question had asked users to think of a problem requiring them to collect and store user information, many of the participants did not select user information or usable privacy and security problems as the most decomposable component of the problem. Whether this was because the user information collection was perceived as a known and understood problem, or because the participants did not separate out the usable privacy and security problems as a domain problem space from the other design problems they faced, was not clear from the survey data.

In the discussions of the technical challenges, some themes emerged that were more directly related to usable privacy and security. One participant noted a technical issue with encryption:

> [We needed a] method of encryption of data that would be secure without being onerous on the systems that used the data for processing. Our systems are enterprise software and services for health insurance companies. It was the storage of credit card information for charges/reimbursements that caused us to review the methods we were using and add encryption to the storage of the data.

Eight of the participants noted that they had challenges with authentication or access, primarily around issues of identity verification and credit card authorization. Examples included the following:

> Verifying the user was really who they said they were. The questions generated by the reporting agency software often confuses people and they wonder why they're being asked these questions. (Ex: Which of the 4 addresses below did you used to live at?)

> There was some complexity around getting the security code given its differing location on different types of credit cards -- not so difficult to do in a [graphic user interface], but more challenging in a [voice user interface] -- and at the time, some cards did not even have a security code.

> Main design problem was updating the customer's personal information when the actual customer present was their spouse. We needed to store the updates, but could not validate them until the actual spouse was present.

All three of these examples illustrate concerns about ensuring that the user was who they said they were, also known as authentication. Before authorizing access for the user, the designer needed to verify the user's identity. Constraints in the design or in the user workflow could make authentication a non-trivial problem. Verification questions could confuse the user. Voice interfaces made the explanation of how to find a credit card security code problematic. Granting rights through requests passed by spouses was both a business process and technical concern.

Designing user flows for simplicity was a common theme in the responses. One typical example read:

> Some projects have complex dependency chains where entering certain kinds of data/values should result in the presentation of differing sets of inputs. Designing the user flow and UI to make these dependencies intuitive or invisible can be a challenge.

In the examples above, we see that one of the primary concerns of the designer was working around the constraints of the design to achieve the desired information exchange or authentication. The basic flow and conceptual model of the authentication or user information exchange was not raised as an issue, but the details of how to achieve that model were often concerns.

Stakeholder Concerns and Business Strategy

In other responses to the same survey question, some participants noted issues within their organization or their stakeholders as being major challenges.

> The challenges were not really on the design side. We were hobbled by management's inability to set a coherent direction.

> Too many decision-makers that made decisions and later changed them. Project scope changed throughout the project. Some of this couldn't be anticipated, much could have been addressed with better and more in-depth planning up front.

> Only stakeholders with significantly different views on how this should be implemented.

Again, to reinforce the point made a moment ago: usable privacy and security problems were not identified as the most important specific challenge for these participants. Instead, the problems were common design issues of requirements gathering and balancing stakeholder needs.

That said, some participants did note the business needs directly related to the gathering of personal information, as seen in the following three examples:

> There were concerns because of the flow of the online application, and the business need to work in additional cross sell opportunities.

> The actual work contained other complexities related to collecting personal information, but they were related to the client's business rules, rather than my design.

> Making clear the distinction between what personalized data you're collecting that remains private vs. public can be difficult. Particularly if users have the option of getting more specific than the defaults in what they do/don't share.

These responses are suggestive of a tension between the business requirements, the amount of data that users were willing to share, and the potential uses for that data. Nissenbaum and others have pointed this out as one of the most basic elements of privacy tension in the online world.

Compliance

Several participants noted compliance with standards and legal requirements as an issue. Two examples follow:

> Some information types have own unique compliance regimen, business logic, and standards that must be adhered to while still operating in a seamless environment to the user.

> Honestly, some of the stuff was not completed because of a lack of documentation I can have confidence in, proving HIPAA compliance on our CMS (Drupal)

Going back to the notion of design constraints, compliance with legal requirements was considered a special case of a constraint, one that involved documentation and business process as much as design and user flow.

Organization Size and Challenges

Respondents who described a technical challenge were sorted by length of time in the profession, design type, primary audience, and organization size to determine if there was any correlation between these factors and the challenges they described. In examining the experiential data, there was some correlation between the organization size of the respondent (discussed later in the chapter) and the type of design concerns seen. Those in larger organizations to struggle with conflicting requirements from different stakeholders. For example, the following two quotes emerged from people working for organizations of 10,000 employees or more:

> There is a tension between what the sales team (recipients of data) want and what they actually need. Analytics show large amounts of drop off in data collection flow, but customers insist on getting large amounts of information. Legal department also has a set of requirements. Finding a compromise that satisfies the client as well as yields a positive, or at least neutral, experience for the customer is difficult.

In this case, the stakeholders (sales team, customers, legal department) have different expectations for the amount of data to be collected in the design. The respondent mixed two terms: "customers" and "clients" for those paying for the respondent's design services, and "customer" for the end user of the design. There were legal requirements for how much data could be collected and different expectations between the client—who wanted large amounts of customer data—and the customer, who expected the data collection to be minimized.

Another respondent encountered a similar dilemma:

> Some information types have own unique compliance regimen, business logic, and standards that must be adhered to while still operating in a seamless environment to the user.

In this case the respondent refers to the stakeholders only indirectly. The "compliance regimen" and "business logic" and "standards" are created by various stakeholders and are potentially at odds with the expectations of the user.

By contrast, participants working for organizations of 1-500 employees reported stakeholder issues less often, and instead were more directly engaged with single stakeholders and well-defined use case scenarios:

> How to communicate to the user when they create their account where and how the information will be used. How to indicate on the page (profile or otherwise) what info is private versus public, etc.

Respondents working for mid-sized organizations reported elements of both depending on the project.

There was no correlation observed between problem description and the factors of experience level, design type or primary audience.

Emotion of the Users

Participants in the survey often invoked themes and concepts related to user emotion and emotional design. "Emotional design" involves the creation of designs with the explicit purpose of eliciting a specific emotion from the user [Castells 2000]. Popularized by Donald Norman in 2003 [Norman 2003], emotional design normally uses aesthetics, branding, and interface choices to evoke specific associations the evocation of specific associations through aesthetics, branding, and interface choices.

Emotional design has been explored to a degree in the field of usable privacy and security [Gefen 2002; Riegelsberger et al. 2005] as a means of evoking feelings of trust, a difficult problem in an online

setting. In the next section, I will briefly describe three categories of responses that touched on issues of emotional design: user attitude, designing for trust, and identity management.

User Attitude

Emotional design literature often deals with the concepts of evoking emotion. In this case, however, the designer knew, based on their scenario, that the users were not approaching the design with a "neutral" point of view. Instead, the user was concerned, perhaps actively annoyed. By implication, one of the major challenges of the design was to bring the user back to at least a neutral point of view, to know that the user's goals had been satisfied even if the user did not appreciate the necessity for the tasks.

One example of a designer who expected users not approaching the design with a neutral point of view wrote explicitly about the user emotions:

> This was credit report related information, so there was a lot of emotion involved on the part of the user -- no one cares about their credit report until there is a problem.

Other participants reported a similar need to be sensitive to user attitude, to the emotion that a user brought to the design. One wrote:

> Changing consumer behavior around the financial account management became difficult, as fear and ingrained behavior blocked change.

Change management, brought up by this participant, involves both making changes to process and helping users to understand the value of those changes. In the case of financial or other sensitive data, change becomes more complex as users are more sensitive to potential threats against the data. This participant cited not only the classic UX trope of "ingrained behavior" but simple "fear" as causing resistance to the desired system changes.

In these tantalizing but short answers, none of the participants gave any hint about how they measured or sought to modify user attitudes in their designs, but it was clearly a concern for some of the participants—and came to the surprise of at least one of them.

Designing for Trust

As predicted in the literature, among the participants, designers' questions of user attitudes led directly to questions of trust: how to create trust, and how to support it. One designer reported:

> Our main consideration was how much information people would be willing to disclose; was the payoff worth the disclosure?

Similarly, one participant noted that their challenge was in discovering "whether users would be okay with providing a full [Social Security Number]." This is a question of user attitude and emotion, and a classic trust question: do you trust this system with your information? More than one of the participants cited the need to "enhance the credibility" or "trustworthiness" of a design as being one of the principle challenges they faced. For example, one participant wrote simply:

> Designing so that trust in the system is ensured is most challenging.

This was perhaps belaboring the obvious, but it was helpful confirmation of one of the assumptions of the study. In the set of working designers who participated in this study, trust questions were an identified, complex problem space. Trust questions may not be the only design issue or even the most vexing, but trust questions were perceived to be of real concern.

One interesting response read:

> Concern about user privacy and whether they would want their location stored. It was before GPS was so widely available, so using a user's location wasn't ingrained in the public's consciousness, and was using a different technology than GPS. Figuring out how to inform the user about the fact that their location was being used in a short time frame over the voice channel (on a phone call) as well as determining how exactly to use the location, especially given that we had varying degrees of accuracy, was particularly challenging.

This dealt, in a breath, with a variety of issues: attitude of the user, prior knowledge of the user, the task flow of the user interface, and more. The design problem was decomposed into elements recognizable to the privacy and security community: location awareness, contextual information for the user, technical constraints. It was one of only two responses to explicitly use the term "user privacy." It was the considered response of the privacy-aware designer to whom so much of the usable privacy and security literature is currently aimed. As such, it was part of a very small minority of responses in the sample.

Identity

While several participants reported on authentication and identification issues — that is, "please prove that you are you" — one fascinating response dove into theory and practice of identity at a complex level. It read:

> Surprisingly the challenges we are facing are not at all what I had anticipated. The biggest challenge we are faced with is that the cloud treats people as people, while most Enterprise platforms treat people as only the professional face of a person.
>
> Lots of trust, security and disclosure problems come up when a person no longer authenticates as their professional self JOE@mycompany, but rather as JOE@gmail.com, their actual self. Mixing personal and business identities is very difficult water to wade through.

As noted in Chapter 2, Nissenbaum [1998] and Friedman et al. [2002] (among many other researchers) have written extensively about the distinction not just between public and private, but personal and professional. The participant mentioned the concept of "personal and business identities," which ties directly into identity theory. Identity theory is a complex subject and mostly beyond the scope of this dissertation, but a brief digression will be illustrative:

Stryker & Burke [2000] call identity "the meanings that persons attach to the multiple roles they typically play in…societies," and further enhance the definition: identities are based on social roles that

we play, expectations attached to the positions we hold in a given relationship network. One identity is the "internalized role expectations" that come from a given social situation. We all contain many identities, "as many as distinct networks of relationships in which [we] occupy positions and play roles."

Key to this notion is the idea that role identities are self-conceptions that we can put a label on [Hogg et al. 1995]. One woman might be a lawyer, a mother, a child, and a dancer. These self-conceptions inform how we interact with the world and, by extension, how the world interacts with us.

Tension arises when one presents an identity to the wrong relationship network, one with different meanings and expectations. When you are anticipating a business interaction with a lawyer, you do not expect a salsa dancer, no matter how artistically talented. Managing one's social identities is a complex and carefully mediated task both in and outside of the workplace [Hogg and Terry 2000].

Identity management online has been described as a series of facets [Farnham and Churchill 2011]. Each facet presents a view of the self without revealing the whole individual. The design problem identified by this participant is an authentication or identification scheme that incorporates multiple facets: a "personal" and a "business" self.

In general, identity management treats the notion of "single sign on," authenticating with a single identity against multiple systems, as a victory for usability. After all, if you are already authenticated, there is no requirement to ask you to re-authenticate again and again each time you go to a new system. However, this designer points out the inherent flaw: if you authenticate only once, then you have only one identity. How then do you select from the identity facets that you want to display?

When was this problem identified? The participant indicated they were "working on bringing a standalone enterprise server platform to the cloud, and that the challenge "was not at all what I had anticipated." This suggests that the problem was identified *during* the design process, as a part of the design iteration, rather than as a constraint or business concern before the design process began. It was

not a problem identified in advance. As with some other types of trust issues, the problem revealed itself only through the design creation itself.

Summary of Experiential Data

Most participants worked on web sites and software interfaces, with a notable majority working on mobile interfaces. A substantial majority of all the participants, 65.7%, had worked on an interface involving a trust question. Of those participants, when asked to recall a specific incident, the majority remembered creating interfaces for use by individuals, not organizations or businesses. The types of data collected varied widely, but nearly always included a unique identifier (81.3%) and often a credit card number (44.8%). Most participants rated the problem as "Neither simple nor complex" or "Complex" (80.2%). Identified challenges included technical problems, stakeholder concerns & business strategy, and concerns about user emotion & trust.

Most participants did not select user information or user privacy & security problems as the most decomposable or important component of the problem. Instead, the participants tended to identify problems of requirements gathering and stakeholder concerns as being the most common issues. That said, trust questions were perceived to be a concern. Where trust issues did come to the fore - e.g. issues of identity management - the problem tended to reveal itself through the process of design iteration, rather than through a pre-planning process.

Resources Used

Finally, participants were asked to select the resources they used to resolve the problem from an available list. Participants were allowed to select multiple answers or write in their own. The results were (n=64):

Table 9: Resources used

Answer	Frequency	Percentage
Searched the web	33	51.6%
Asked a mentor or supervisor	17	26.6%
Asked a co-worker	29	45.3%
Consulted a reference work	25	39.0%
Adapted an existing solution	35	54.7%
Relied on your own design experience	50	78.1%
Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).	17	26.6%

An overwhelming majority (78.1%) noted that they relied on their own design experience. That fits with Cross' model of expert design [Cross 2004]: the more experienced the designer, the more the designer will rely on their own experience rather than seeking counsel from others. As noted earlier, the participants in this study were more likely to be experienced designers than new to the profession.

Just over half the participants (51.6%) indicated that they searched the web for information or a solution.

Seeking help or guidance from a co-worker (45.3%) was much more common than asking a mentor or supervisor (26.6%). This suggests that peer advice is as important to these designers as input from their mentors or management chain, if not more so.

Demographics

As with any study, one of the primary concerns of the survey was to gauge the quality and reliability of the sample. For this purpose, the study included a number of demographic questions. The results of the demographics questions will be discussed below.

Role

The survey asked participants to identify their professional title by asking: "What title would be listed on your business card?" Participants were given a short free-text field to enter their answer.

Responses were varied in nature but did show some consistency in themes. 33.1% of respondents indicated that their title included "user experience" or "user interface" or "UX" or "UI". 25.5% of respondents indicated that their title included the term "design." 17.2% of respondents indicated that their title included the term "web." More examples follow in the table below.

Table 10: Example phrases from professional titles

Title	Respondents	% of Respondents
"User Experience", "User Interface" or variations	48	33.1%
Web	25	17.2%
Architect	11	7.6%
Lead or Manager or Director or VP or CEO	25	17.2%
Design	37	25.5%
Specialist	18	12.4%
Information	7	4.8%
Usability	14	9.7%
Professor	4	2.7%

Note that these responses are not mutually exclusive. Three respondents listed their title as "UX Designer," for example. Note also that these words given in this table are by no means exhaustive. Unique titles included "Research Psychologist" and "Business Analyst" and "Admin Assistant," among others.

17.2% of respondents had a job title suggesting they were in a leadership or management role — "manager," "lead," "VP," or "CEO."

Experience Level

The survey asked two questions to gauge the design experience of the participants. The first question asked how long the participant had worked in their *current position*, while the second asked how long the participant had worked in their *profession*. The results are shown below.

Table 11: Duration of position

Answer	Frequency	Percentage
Less than 6 months	22	15.0%
6 months - less than 1 year	9	6.2%
1 year - less than 5 years	63	43.2%
5 years - less than 10 years	27	18.5%
10 years or more	25	17.1%

Table 12: Duration of time in profession

Answer	Frequency	Percentage
Less than 6 months	2	1.3%
6 months - less than 1 year	4	2.7%
1 year - less than 5 years	20	13.7%
5 years - less than 10 years	29	19.9%
10 years or more	91	62.3%

Survey participants tended to be experienced in design. 62.3% reported that they had worked as designers for 10 years or more (n=146). 43.1% reported that they had worked in their current role for 1-5 years (n=14).

These results suggested that, at least based on length of time in the field, there were few "naive" and "advanced beginners" in the survey. I use the terms as defined in Dorst's model of expert design [Dorst 2008]. Dorst's model of expertise is based on design practice rather than length of time in the profession, so this is not a perfect match to the model. However, Dorst acknowledges that expertise develops with experience in the field. Less than 4% of the participants had worked as designers for less than a year. Most self-reported a lengthy term of industry experience.

In this data set, experience level was not significantly related to the likelihood that the participant had encountered a problem involving a trust question ($r(144)=-.02$, $p=.78$) or the complexity rating of trust questions ($r(94)=.05$, $p=.60$). It is possible that this is related to the low number of "naive" and "advanced beginners" in the survey.

Forums

One additional optional question was asked of everyone who took the survey: "What are your favorite professional e-mail lists, forums, or other online networking locations?"

The primary purpose of this question was to aid the snowball sample. The results were used to find additional potential online fora that would be fruitful grounds for recruiting additional participants in the survey.

One unexpected additional result of this question was the difference between participants who identified lists that were directly associated with professional associations such as CHI or IXDA, versus

public social networking sites such as Twitter or LinkedIn, versus other independent channels. Several participants included online locations from more than one category.

Table 13: Participants in forums

	Total N	Professional org	Social	Other
Participants	100	27	38	84

Professional associations were identified as those organizations that specifically identified themselves as organizations of professionals requiring a paid membership. Within these results, these organizations were: ACM CHI or SIGCHI, iXDA, UPA, ASIST, UCDA, and AIGA. Public social networking sites were Twitter, LinkedIn, Facebook, and Skype. All other responses were recorded as independent channels.

The results suggested that more local, independent forums may be more commonly used in this population for online professional networking than non-professional social networking sites or those of professional organizations. For the purpose of promoting usable privacy and security information and learning, this suggests that a more distributed approach might reach more individuals within this population. It should be noted, however, that the sample size was not large enough and not structured to allow for full conclusions to be drawn.

Organization Size

The survey asked a yes / no question: Were participants consultants or self-employed? 24.5% of the survey participants worked as consultants or were self-employed (n=143). The remaining 75.5% were assumed to work full-time for a single employer.

A second question asked all participants for the approximate size of the participant's current employer. The values were presented on a Likert scale (n=146):

Table 14: Approximate size of current employer

Answer	Frequency	Percentage
Less than 100 employees	40	27.4%
100 - 500 employees	19	13.0%
501 - 2000 employees	15	10.3%
2001 - 10,000 employees	20	13.7%
Over 10,000 employees	52	35.6%

In the earlier question, 35 participants (n=143) said that they were a consultant or self-employed. "Consultant" or "self-employed" in this context implies simply that the participant is under contract with multiple business entities at once, rather than a single entity. Would these participants be part of a larger consultant organization like Deloitte, or a small or individual organization. There was a subtlety here that should be explored. A self-employed designer has autonomy and agency, and the authority to make design decisions appropriate within the constraints of the identified client needs and budget. A consultant working in the context of a larger organization often does not have the same level of autonomy in their design decisions.

To learn more about this question, the participants who identified as a consultant or self-employed were analyzed separately for employer size from the remaining respondents. The answers of those 35 participants to question #6, asking them of size of their current employer, are reported below.

Table 15: Consultant / self-employed organization size

# of employees	<100	100-500	501-2000	2001-10K	Over 10K
Respondents	24	2	4	0	4

The majority of participants who self-reported as consultants or self-employed reported themselves as working at an employer of "less than 100 employees." However, 17.1% indicated that they worked for a larger firm, and 4 indicated that they worked for a firm of over 10,000 people. (No participants who self-reported as consultants stated that they worked for a firm of 2001 − 10,000 employees.)

For the rest of the participants, a majority worked for firms with over 10,000 employees.

Table 16: Other UX designers' organization size

# of employees	<100	100-500	501-2000	2001-10K	Over 10K
Respondents	16	17	11	20	48

Age

The age distribution of the participants was as follows (n=146):

Table 17: Participant age distribution

Age Range	18-24	25-34	35-44	45-54	Over 55
# of respondents	4	39	52	30	21

Over 62% of the participants were between the ages of 25 and 44. As the population was of working professionals, this sample made intuitive sense. The sample showed a natural bell curve with the largest portion of respondents in the 35-44 age range at 35.6%.

The sample included only four people in the 18-24 age range. This also seemed reasonable as the sample was designed to look for professional designers with working experience, explicitly excluding students or trainees.

Gender

Participants were asked to identify their gender. This was an optional question but had a very high response rate (n=145)

76 of the study respondents self-identified as male while 69 of the study respondents self-identified as female. A goodness-of-fit chi square test revealed that differences in gender in the sample were attributable to random variability. There was no significant difference in gender among the study participants (n=145, Chi Square (critical, df=1) = 3.841). This was reassuring as it indicated that there was no significant bias for gender in the sample.

Table 18: Age goodness-of-fit test

	Male	Female	Total
Observed N	76	69	145
Expected N	72.5	72.5	145
Chi-sq. stat	0.168965517	0.168965517	0.337931034
Degrees of freedom = 2-1 =1			
Chi-square(critical, df=1) = 3.841			

Reliability

I noted earlier that the demographic questions were intended to help understand the reliability of the data. What conclusions regarding reliability can we draw from the responses to these questions?

Gender was not a significant factor in the sample. Age, role, and time in profession all tended to indicate that the sample largely represented an older, more experienced set of designers. This was as intended. The survey call and snowball sample strategy were both designed to attract experienced and expert designers over those in school or new to the profession.

The advantage of a more experienced sample of designers is an increased likelihood that the participants would have seen and worked with trust questions in their daily work. A majority of the participants did in fact work with trust questions, providing valuable data.

The sample showed a variety of job roles across a range of organizations and organization sizes. Self-employed designers and consultants were represented by roughly a quarter of the sample, a respectable minority. No organization size was represented by more than 35% of the sample, which suggests that the sample included designers who worked with a broad variety of organizations from small business to large enterprise.

We see, therefore, that the snowball sample was an effective strategy in terms of providing a variety of viewpoints and design experiences from a diverse population.

Summary

The sample set for this survey tended towards designers with extended experience. A large majority of them reported that they had dealt with personally identifiable information (PII) in one of their designs.

One of the characteristics of the usable privacy and security design literature is that the problem space is often considered to be especially complex, worthy of deep study and a unique set of knowledge and skills [Ackerman and Mainwaring 2005; Barth, Datta, Mitchell and Nissenbaum 2006; Cranor and Garfinkle 2005]. One of the chief findings of this survey is that, in fact, the problem space is not as unique as the literature might imply. Common technical design problems or interaction design problems were mentioned much more frequently in the survey than issues of usable privacy and security.

That said, it is suggestive that such a large percentage of designers in the survey reported that they had worked on designs requiring personal information from the user. It suggests that usable privacy and security problems are in fact a common issue in user experience design. Usable privacy and security issues are directly relevant to the majority of user experience designers.

With that said, the data reflects the reality that user privacy is one of a range of design problems facing the working designer at any time, and not necessarily perceived to be the most important issue. How, then, can the usable privacy and security community influence the designer's choices?

Over half the users searched the web for answers to their usable privacy and security problems. A future study might inquire more deeply into these searches.

One clear pattern that emerged was the notion of consultation. A majority of designers asked other designers for guidance, either peers, supervisors or mentors. This is in line with findings from the existing design literature. It suggests that, where possible, targeting thought leaders and experienced designers in an organization with information about good usable privacy and security practices can have a positive "trickle-down" effect on the organization as a whole. As knowledge is disseminated from hand to hand, the usable privacy and security work of the organization becomes stronger. Contrariwise, if one's peers are poorly informed about or disinterested in usable privacy and security, the organization as a whole may see reduced usable privacy and security "good" behaviors.

By itself, the survey was interesting but could give only hints to some of the research questions that the study was interested in: when and how usable privacy and security problems are defined and decomposed during the design process. For further insight, I now turn to the follow-up interviews performed as a complement to this survey.

Chapter 5: Interview Results

In this chapter, I will examine the results of the semi-structured interviews performed as a complement to the earlier survey of designers.

Demographics

In total, there were six interviews conducted. One of these was removed from the data set at the request of the participant, who was concerned that she might have revealed confidential information from her employer. This left five active participants.

The domain of work for each of the participants was varied:

Table 19: Demographics of interview participants

Participant	Domain
1	Financial / insurance
2	UX consultant / speech UI design
3	Research / academia
4	Non-profit
5	Financial / bank

All of the participants reported that they had at least 10 years experience in their profession. Four of the original participants were men. One was a woman. All lived in the US. Two were located in Seattle; the others were based elsewhere in the country.

I interviewed participant 3 in person. I interviewed all of the other participants by phone. In both contexts, I used the same interview protocol. There is a possibility that my gender (male) and race (white) may have influenced the potential of receiving socially desirable responses, which I attempted to partly

mitigate by using phone interviews and interviewing exclusively about organizational and workplace practices [Moorman and Podsakoff 1992].

To strive for a representative sample, the participants were selected in part based on their responses to the short answer survey query asking for details of the design problem they encountered. Based on those short answer queries and the data from the resulting interviews, I will briefly describe the background of each of the participants.

Participant 1 was an enterprise architect and developer for a major health insurance provider. He was one of the most technically knowledgeable people in the group. Based on his responses in the interview he also appeared to have a great deal of agency as a designer over many aspects of the system, not just an individual component or feature. However, because of the nature and size of the enterprise that he was working with, his designs were constrained by compliance and regulation needs as well as by the influence of many stakeholders. He also worked with a sizeable project team of different disciplines with a variety of components. The primary focus of the interview was a combined technical / usability challenge regarding encryption of credit card data.

Participant 2 was a user experience designer who focused exclusively on speech and voice user interfaces. He also was highly experienced in his field. He was responsible for developing the vocabulary, scripts, and user flow for speech interfaces for a variety of different clients. Within the scope of the voice user interface, his design influence was substantial, but he did not describe the ability to set user goals or otherwise influence designs on a more strategic level. He typically worked with large enterprises such as banks and telephone companies.

Participant 3 was a university professor, for whom design was a professional and personal interest but not a primary source of income. By Cross' definition [Cross 2004], therefore, he was closer to a novice designer than any of the other participants, though very experienced in his profession and familiar with the principles of user experience design. Unlike the other interview participants, he had sole agency and

responsibility for the designs he created. His design challenges typically revolved around web sites and related databases for use by academic or research groups.

Participant 4 was a web designer and usability consultant who worked for a small-business firm, typically on projects that did not involve large time investment or budgets. The project he described in the interview related to a web site for a non-profit opera company. The primary constraints he described were around client requirements and budget rather than stakeholders or other team members; he had a great deal of autonomy in creating his designs.

Participant 5 was also a user experience designer working for a major bank on the east coast of the United States. She primarily worked on web application interfaces but also had an interest in mobile interfaces. Of the interview participants, she reported the least agency and ability to influence her own design work due to constraints by management, stakeholders, and other project members. The design challenges she described primarily involved convincing management and other stakeholders to fund or support her ideas.

The participants demonstrated variety in several areas: the type and size of organization they worked with, the amount of agency they had over their designs, the type of designs they were creating, their professional background, and their level of technical expertise.

Themes

As discussed in Chapter 3, the interviews were transcribed and the transcripts assessed for emergent themes. In keeping with the structure of the interviews themselves, I will use the discussions of design process to lead into the subject of usable privacy and security.

The primary themes that emerged from the interviews were:

Defining the problem space. This theme spoke to one of the key questions of the study: how designers defined the problem space around usable privacy and security, both in conception and in practice.

Defining audience. Any designer must consider the audience for the design while working through any design problem. That designer's mental model of the audience has a strong impact on the designs created. The interviews allowed for an opportunity to learn more about how the participants were defining the audience for their designs involving trust questions.

Trust and security. To reiterate an important point, trust issues are related to but separate from technical security issues. Technical security issues are about the creation of controls and mitigations against a specific, identified threat. Trust is a conceptual relationship between a person and an entity. The interviews revealed important points about both.

Decomposition and modularity. In the survey chapter, we noted that the participants often did not "modularize" usable privacy and security problems into a separate conceptual space as part of the design process. The interviews provided more evidence to show this lack of modularization.

I begin with the issue of defining the problem space and decomposing the problem.

Defining the Problem Space

Recall that one of the research questions for this study was: *For the designers studied, how do they define their problem space and their audience*? I use the idea of "conceptualization" to encapsulate the participant's description of this process of audience and problem definition. Both are key elements of design [Dorst 2008; Zimmerman, Forlizzi and Evenson 2007] and have a direct and practical impact on the usable privacy and security of that design [Yee 2005].

"Design is iteration," says a common trope in the design field [Mosborg et al. 2005]. One of the implications of that statement is that comparatively few designs are begun from scratch, with a blank

sheet of paper. Designs are typically iterations on a previous design or use elements of previous designs, a phenomenon so common that Goel & Pirolli gave it a label: "reversing the direction of the transformation function," or explicitly trying to change the problem situation so that it more closely fits prior knowledge and expertise [Goel and Pirolli 1992].

In this sample, only one of the design examples given by a participant was a new design, a web site built for an opera company. The remaining examples were iterations on previously existing designs. The changes to the design were additions or modifications, rather than a new creation. These changes typically fell into three categories: new *activities*, new *requirements*, or new *context*.

I use the term *activity* in the sense given by activity theorists [Kaptelinin and Nardi 2006] and interaction experts such as Don Norman [Norman 2006]: an activity has a subject (the user), an object (the user's objective), actions (tasks), and operations (routine subtasks not requiring attention.)

As noted, in the case of the non-profit, the design and the activities were new, not an iteration of a previous design:

> The opera [company] needed some system by which patrons of the opera could donate online and become a funder in that they wanted it to, you know, not just say thanks very much, but kind of tier the funding and give feedback as in they could sponsor specific things for example, so basically, they could see what they were funding rather than just anonymously handing over a check and saying thanks for the money.

In this case the design was not an iteration but a brand-new design, sometimes called a "green-field." In a green-field scenario, the designer has maximum freedom within the constraints of the user tasks and client's wishes to create a design according to their expertise.

This was not the case every time, however. Activities were sometimes linked to a technology upgrade, a case of adding features and functionality to a system that was already being modified for reasons of technology constraints. For example, the professor explained:

> There was a project that had been done by a colleague, and the technology that supported it was dying. We needed it to be re-hosted and along the way, a variety of affordances were identified that clearly seemed to make sense because the bylaws of the organization, we had an obligation to publish

> a directory and it was felt that we could do that as a public access level of access, and clearly as membership coordinator and so on there was a need for a kind of administrative level that had no holds barred in terms of what was there and in between, it was felt that, partly because the earlier implementation had included it, but it was felt that it was reasonable to give the users some management control of their own visibility in order to make it visible and to whom.

In this case, the new activities of directory administration and user profile control were to be added as a side benefit of the technology upgrade. However, in our discussion of the resulting design problem space, the new activities were the focus of the design challenge. The activities became the central problem space of the design, and the design was an iteration on a previous implementation.

In other cases, the activities remained the same, but the requirements had changed. The designer for the insurance company explained:

> What changed, though, is the government regulations of how that data is stored and handled in the back-end systems in order to make it secure and less able to be accessed by people who shouldn't have it…. The things that come from federal and state governmental agencies where the government says you must do this in order to operate are 'must haves.' We do our best to put those enhancements into the system well in advance of the regulatory deadlines so that our customers can accept that enhancement and upgrade their system before the regulation deadlines hit.

In this case, the changes to the existing design were driven by the need for compliance with government regulation, an external constraint imposed upon the design process. The design challenge, as expressed by the participant, was to take an existing design and modify it to satisfy the pre-existing business requirements and the new regulatory requirements while still providing a quality experience for the system's user.

Finally, there were cases in which the activities and requirements remained unchanged, but the context of the design was different. The designer of voice-driven interfaces explained:

> But, you know, you probably have paid by phone once or twice– so there's a standard of bits of information that you need to collect and in this particular case, this was – let me think – probably around 2000 – 2001, something like that. So, those hadn't been – they weren't as ubiquitous as they are now. And then, you know, of course trying to design this for use with a speech system rather than a touch-tone system, it was already running as a touch-tone application, so the goal here was to change to speech and try to smooth things out.

In this case, the activities of the user and the requirements of the design remained unchanged. Only the input method had changed, from a phone touch-tone system to a voice recognition system. That change in input method changed the *context of use*, requiring a substantial re-work of the previously existing touch-tone design. Similarly, for the financial participant, a change in context from a desktop-based web browser to the constraints of mobile devices caused some design challenges:

> One project I'm working on right now is mobile banking. And that one's been a real challenge for me because I haven't done anything with mobile banking before, so there's a lot of challenges that go with it, I mean, you're dealing with, you know, the tiny screens of a feature phone, you know, the iPhone and the Android and the Blackberry and all the different – and then there's the iPhone II, and every Android can have the Android operator and then the Blackberry uses the little wheel vs the ones that are touch, so there's just a lot of , it's not like you can design just one kind of wire frame and do it.

We see overall that the common themes in the conception of the problem space were around design constraints, iteration, and stakeholder input. Where usable privacy and security was mentioned in the conceptualization of the design, it was mentioned in the context of regulatory requirements rather than as a feature or concern in its own right. Both of these are indicative of how designers structure and conceptualize usable privacy and security problems in their work.

Defining Audience

Designers define their audiences in ways that guide and inform persuasive design, providing structure and a shared sense of goals and purpose [Fogg 2002; Johnson 1998; Ong 1975; Winsor 1998]. The ways in which designers define their audience shape their design decisions, both decisions relating to usable privacy and security and other domains. With this in mind, how did the designers in this study define their audience?

The financial designer defined their audience by their economic status and access to certain technology.

> The bank I work for is always kind of going for the higher end consumer, but now, of course, with the economy being in the state that it is, they had a lot to do with it, as well, and you've got to broaden your customer base and in order to do that, you have to be able to, you know, provide offerings that are going to entice people, you know, not only from the wealthy, probably upper class type of people, but you want people who are going to be taking – the up-and-coming people, as well.

The same participant explained that their new target customers were expected to be using mobile devices rather than computers, for reasons I will explain in the next section. A different participant followed up on the notion of how and whether device ownership can be used to identify interesting aspects of a market segment:

> It's like iPhone people are using it more like an aesthetically-pleasing device, but if you look at the Android, a lot of the applications are different than some of the iPhone ones, and so it's just interesting to--there's no set audience. You know, you've got, I mean iPhones either can be pretty much anybody; Android's probably going to be people 18 to 25, but there are people 35 that use Androids, and 40-year-olds, you know what I mean?

The second quote tries to pair trends in technology with demographic trends in the technology user. For example, the participant theorizes, young people more commonly use Androids, where iPhones might be used by anyone. The designer for a non-profit was more explicit about why the age of the user might matter:

> Some people who might be funding this kind of a cause or organization are likely to be in an older demographic. It was opera-related – it tends to be an older demographic – so we had to kind of make it as simple as possible and not too many bells and whistles but at the same time sophisticated enough so that we could get information processed and user identified.

Knowledge of the potential users led to certain design constraints and prioritization: simplicity over features, positive *anshin* as part of the experience [Yamamoto et al. 2011].

The architect used their knowledge of their user groups to validate their requirements and design, as seen below. Again, we see that the definition of audience plays a key role in the design.

> Most of our users, for the most part, are – the customer service users, we have a very good feeling for. We have a customer service user group that we communicate with regularly and they give us enhancements for that area of the system, so the business application designer was in touch with the customer liaison and very familiar with the services represented so we made sure that that user

> community was well-represented in the design phase. And then the system-to-system communication was much more straightforward, because you didn't have to really talk to anybody.

Finally, in the case of the academic designer, he was himself a member of the group he was designing for, and he personally knew all of the other audience members. When asked about user research or audience analysis, he commented:

> Sure, sure – not active user research, not surveying the members and finding out what percentage would be interested in having what features, because I suspected there would be very little feedback. I'm pretty sure that I emailed the membership and said if you have anything – any suggestions about the old system that you'd like to throw away, I'd like to hear them. I don't think I got any responses. And certainly, the guy did the first system – he is a friend of mine – so I shoot him an email and say we got another whack at this so take a look at it. Operating system and browser quirks I would usually sort of ask a slew of folks to just take a shot at it to see if Internet Explorer was doing anything particularly weird with rendering of things and stuff like that, periodically.

As we can see, not all of the designers in the survey reported a rich audience analysis. The type of analysis performed, and the depth to which the audience was defined and understood, varied widely from project to project and designer to designer, even in this small sample. This is a potential area for further research in the field. Current usable privacy and security research focuses largely on user flow and choice related to particular tasks. Is it possible that emphasizing quality audience analysis research and practices would improve our understanding of how to positively influence design for usable privacy and security?

Where performed, the audience definition was largely done as a market segmentation exercise, thinking about marketing orientation [Mohr et al. 2005]. As audience definition is a key component of structuring a design problem [Goel and Pirolli 1992], its absence in some of the responses was a surprising finding.

Trust

As noted elsewhere in this dissertation, trust is not exclusive to the user. The organization or system must trust that the user is who they say they are, and that the user will follow through on any promises that they make [Cofta 2007; Riegelsberger, Sasse and McCarthy 2005]. As an example, one designer pointed out that their system collected varying amounts of user information depending on the level of pre-defined trust in the user's identity:

> It depends on what kind of client you are. I mean, it could be your account number. It could be a debit card number, it could be a PIN number. It's not your Social Security Number – well, for certain types you might have to have a Social Security Number, and, like your ZIP code and then you create your user ID and password. For – if you're like a client who we can't ascertain your identity because we don't have – you don't have an account number and a PIN number, because you don't have those, then we just send you to Lexus Nexus, so there's a lot of information that needs to be collected to make sure that you are who we think you are.

In this case, the designer's implicit assumption was that they only wanted to collect the information they needed in order to satisfy the authentication requirement. Once they had enough to authenticate the client to their satisfaction, the level of trust in their client was established.

We have seen a common thread in the usable privacy and security literature is the ethics and potential loss of trust involved in collecting too much personal data, or using personal data in ways that were not obvious or not to the benefit of the user. Two designers made implicit reference to the potential ethical and security concerns of collecting more data than they needed. An example of a security concern was:

> I don't think we had any concerns as far as that because we actually were collecting – it was something that online banking was already doing, so we were just piggy-backing on that process, but I do remember back when I was doing online account opening, that there was a real concern that, at the time, you know we were making up numbers like a Social Security Number and a PIN, or something like that and there was a real push to get people to, you know, to move people away from having to find their whole Social Security Number. Or even the last five of the social – you can find other identifiers besides that. And the same thing with a 401(k) application, you know, we moved everything away from the use of the Social Security Number and a PIN to you know, creating a user

> ID and password as your log-in credentials. Some of the older systems, you know, were looking for different types of credentials to work with, that were too sensitive to be asked for on a regular basis or transmitted on a regular basis, you know, just for the logon.

Another example was more ironic:

> There wasn't really data mining going on, we weren't being Facebook about this. It was purely just so they could process the financial transactions. There wasn't anything other than that. Also so they could send out marketing, which we had opt-in options for.

"The right to be left alone" is a long established principle of privacy [Gilman 2012]. The respondent's comment that they collected personal data "purely so they could process the financial transactions" was undermined two sentences later by an admission that the data was used for marketing purposes as well. It is important to note that opt-in marketing is a legitimate use of user information under American privacy law, so this was not a case of breaking rules. However, there is an implicit assumption in the way the respondent phrased their answer: "purely for financial transactions" includes data for marketing purposes simply as a matter of course.

Trust is built in part by a sense of shared expectations: the knowledge that the trusted party will act in the way that you expect them to. A trusted party that collects information "purely" for transactional purposes and then uses the data for marketing purposes may not remain a trusted party if the details of that extra use are not clear to the user. For the designer to speak to the issue as they did suggests that their conception of trust may not be as strict as a privacy advocate's.

One unexpected example of a trust issue came up in the bank designer's discussion of their audience:

> There's a large Hispanic population here and they're called the under bank, which means they've got money, but they don't trust banks, and so they do a lot of things with their mobile phones like, a prepaid card and they don't want to get onto the computer and they don't want, you know, there's also a lot of people that will buy a mobile phone but can't afford a computer.

The respondent's cultural / racial labeling of the audience in question is possibly over-simplified at best if not actively problematic. To remove potential bias from the discussion, let us consider this audience segment as "under-served," acknowledging that the cultural / racial label may or may not be

fully accurate. The under-served audience, according to the bank designer, begins with a low level of trust of the organization. Nissenbaum [2004] points out that trust in an organization does not happen in a vacuum. It is based, among other things, on an established reputation, and built on all the interactions that the user has with that organization regardless of channel or venue. In this case, the level of trust in the organization by a particular under-served population is low. Consequently, members of this audience use bank services in ways that they perceive to be safer: for example, using pre-paid debit cards rather than cards that draw from a banking account.

The under-served audience may also not have regular access to a computer. Instead, members choose to use mobile devices. The implication for the designer is that completing scenarios allowing for exclusive mobile banking becomes a key element in building trust with this audience. However, the designer's management resisted the idea:

> I had a lot of resistance to getting any – bringing up the idea of people being able to do it – to do enrollment in their mobile device, to enroll in mobile banking…. If I'm going to do mobile banking, I want to be able to enroll in mobile banking and start using it, and so as I was working through, like the computer version of it, you know, the one that you would do on a desktop or laptop, or whatever, it was like, okay, well there's really no reason that we can't do, you know, these things, you know, via the mobile device, and they're just like, you know, they're not going to want to do, I mean a real spot, that they wouldn't want to deal or do that.

Cofta [2007] and Riegelsberger and Vasalou [2007] both note that trust is built or lost through many moderated interactions, not just a single trust decision. The designer shows awareness of this problem. Having analyzed this audience and determined that they use mobile phones exclusively, the designer asks: why would we not enroll in mobile banking through the mobile device that the audience members use and trust? In Gefen's [2002] terms, it builds confidence in ability ("we can help you"), benevolence ("using the means you have and are comfortable with") and integrity ("without forcing the interaction to be on our terms.")

The resistance from bank managers towards enabling a fully mobile-phone-enabled scenario is also interesting when viewed through the lens of social construction of technology. The managers assume, and the technology built assumes, that major online banking operations will be done through the use of a web browser on a computer. Whether for economic or other reasons, this particular audience eschews the use of computers in favor of using the mobile phone exclusively. The mobile device becomes the mediating device for *all* aspects of communication with the bank, something that the bank managers did not expect or intend. [Kline and Pinch 1996]

The findings here emphasized that trust issues are common issues in design. The nature of the design concerns around trust varied depending on the stakeholders' attitudes towards the actors and activities in question. An interesting side note was that only one participant *explicitly* mentioned trust, in their discussion of whether or not their customers would trust a bank. For other participants, comments about trust were implicit and hard to tease out. This is a useful reminder that even for experienced designers, trust questions are not easily separated from other concerns in design.

Security

We have seen that technical security issues are conceptually separate from trust issues for the purpose of this study. This is an important distinction because technical security issues are easier to tease out and review as a separate entity. For technical security issues, several designers displayed an in-depth knowledge of specific security technologies, threat mitigations, and design concerns — not on an activity level but at the level of individual sub tasks or technology interfaces. One case in point ran as follows:

> So, one example is – the actual requirement was to encrypt the data at risk, right? So, somebody enters a – well, we have a debit card – if the number is known to the person entering it, by the time it leaves the user's fingers and when it gets stored in the data base, it gets encrypted in a way that is no longer recognizable or easily connected. So, we were encrypting the data at risk in just one field, not the entire record. Encrypting the entire record would introduce significant negative performance complications. Basically, it would make the server slow as molasses–so, that wasn't an option. We did

> discuss, you know, basically encrypting the whole record and that was just, you know, even though the security people wanted us to do that, that was just not a viable solution.
>
> So, the method of encryption was really up to the design and architecture, you know, the common components team, to determine what specific method of encryption we could use within the industry that would meet the regulatory requirements and, you know, the deliver mechanism. You know, we didn't want to write our own encryption method. So the fine-tuning of the design came in to – we understand that it has to be encrypted when it is written but at what point do you unencrypt it? Do we send it to the external system or the banking system encrypted or along with the key and then they unencrypt it? So, do we give them a copy of our component and we give them the data plus a key and they use it to unlock the value? Or do we de-crypt it – unencrypt it – and then ship it? I mean, that seems like a simple decision, but that was probably one of the most time-consuming decisions we had.

We see here several classical elements of a security design problem. There is a threat (data at risk of exposure) and a mitigation (encryption). There is a security trade-off based on design constraints: The most secure solution would make the server response time unacceptably slow, so a compromise was required. Given these constraints, there were technical details to be worked out over exactly where and how in the process flow the encryption and decryption should be performed.

Usability is a peripheral but important part of this participant's discussion. Server response time is about ensuring that the database server appears responsive and performant. The user should not have to wait for a transaction to be completed. In this case, the usability issue is not about the potential of user error or confusion, but the potential for the user to find the solution to be an unacceptable burden. Saltzer and Schroeder [1975] would have recognized the problem immediately.

Note, however, that the participant saw this as a security issue, not a usability issue. The whole discussion is framed in technical terms of how the data is treated by the back-end systems and in the communication channel. The participant did not make direct reference to the user's experience in their description. This was a common theme in the discussions of technical security issues. Another participant spoke of a similar problem in regards to the particular encryption method they had chosen:

> So one of the – one of the unfortunate parts of it was we actually got probably seventy-five percent of the way through the construction phase and we discovered that we couldn't use the encryption

> method that we had picked according to current industry standards. We didn't really change our methodology, but the reason we couldn't use it was because it would sell to the international marketplace. The encryption method that was currently preferred in the United States is actually protected under government secrets, probably the wrong thing, but basically, you can't export it. So, we couldn't go out the door with the solution that we first wanted, because we couldn't export it and therefore we would need an alternate solution for international customers, which was just not an acceptable or workable solution, so you know, we sort of keep our eyes on it, waiting for something to change and go back and look at it.

In this case, the concerns are purely about regulatory compliance and ability to sell internationally, rather than anything directly related to user experience.

The academic did make reference to the user in mentioning a technical security problem, but it was in a different context:

> One of the features we never did implement, partly out of security concerns, was the ability to take an ad hoc query and execute it and which would have allowed a savvy membership coordinator to, you know, find things that weren't built into the software, and in fact, I'm not sure that any of the membership coordinators have been that savvy that they could be trusted with SQL syntax without mangling things. I wasn't sure how I wanted to handle the security in it, so not being sure, it doesn't happen.

Structured Query Language (SQL) is a powerful and flexible language for interacting with a relational database. A properly constructed SQL query provides rich abilities for gathering and sequencing data. However, SQL queries can also be used to modify the underlying data tables, creating the potential for data loss if the queries are mis-used.

"Membership coordinators" in the participant's discussion filled a role commonly referred to by IT professionals as an "edge administrator." The coordinator has administrative rights to modify the data in the database, in the interest of keeping the membership lists up to date. There are limits to this database administrative power, however. In this case, the system designer did not believe that the coordinators "could be trusted with SQL syntax without mangling things." They could be trusted to modify the data in

a table, but not the database tables themselves - not through malice, necessarily, but simply because malformed SQL queries had the potential for causing damage.

Returning to the language of Cofta [2007] and Riegelsberger and Vasalou [2007], the system—and the system's designer—must trust that the user will follow through on any promises that they make. In this case, the implication was that the designer did not trust the user to follow through—to avoid causing damage through error. It is a security problem, in the sense of security as a means of granting authorization and permissions, but also a trust issue: exactly how far does the designer trust the admins of their system?

Three of the other participants in the study made no reference to specific technical security mitigations in their discussions. One summarized the thinking:

> We were very well-versed in using the secure systems for collecting that information and making sure it wasn't anything that was prone to identity theft or anything like that. That was more the software developer's world. If there was a concern I never heard about it, basically.

In other words, the responsibility for dealing with any technical security issues fell on others in their development team. It was assumed that the technical security issues were either already solved through prior art, or that they would be resolved by the developers.

In all the cases mentioned here, technical issues were an easily identified set of concerns that could be resolved with technical, code-level fixes. Technical security issues typically did not revolve around or concern themselves with user interaction except when the mitigation for the user interaction resulted in an unacceptable decline in usability for the customer.

Decomposition

One of the questions of the study dealt with the notion, taken from Goel & Pirolli [1992] and Langolis [2000], of how the designers "decomposed" their design problems. Given an activity that the designers were attempting to enable, how did the designers conceptualize the design problem into logical subunits that could be analyzed, framed, and addressed in a design? What is the conceptual model that designers apply to their design process?

We have already seen that trust issues were difficult to tease out — decompose — from other concerns in the design process. Technical security issues could be modularized and dealt with separately but typically the impact on the user was not considered or was considered minimal. Participants often considered the technical security issue to be a concern of someone else.

The speech user experience designer used the concept of a speech "grammar" - recognized terms, decision trees, and cue words - to decompose a design problem:

> What happened on a different project – this was a reservation – this was for doing reservations, and it turns out that for reservation systems, well, you know, there are some complexities associated with midnight. That's the zero. So, what do you say, if someone says they're going to pick something up at midnight, then you know, that makes the date ambiguous in some ways. I mean, they'll tell you the date, at midnight, and you're still not sure, but – so – but another thing that happened was, you know, you can't have a reservation system the first time through, we built the time grammar, so that, you know, you'd ask the person, you know, when are you going to pick up the car? And you know, somebody will say 11:30 a.m. and that works fine; or say, 12:30 or 2:30 p.m., that works fine, too. But it actually turns out that people get a little uncomfortable with Twelve, so rather than say "12" if they're going to pick up at noon, you know, quick, they say is that 12:a.m. or 12:p.m. You've got to think about it a little bit, so they just say "Noon" and I didn't have that in the grammar, so easy to fix.

While this example is not specific to the usable privacy or security domain, it is a tidy encapsulation of a method of decomposing a design problem. The overall goal for the activity was to place a reservation on a rental car. This was decomposed into a set of tasks, including the one cited here: allow the user to indicate the approximate time when the car would be picked up. Because the system was meant to use a

speech user interface, the designer created a formal, pre-defined script for explaining the user task and a "grammar" of acceptable inputs. There was an observed usability problem with the task - what if the user wants to set the time to midnight or noon? The fix for the usability problem was to alter the accepted input, the "grammar" and possibly the script as well.

Represented here are several elements of Goel and Pirolli's model [1992]: the modularity and decomposability of a design problem (specified tasks), the control structure (speech input and grammar), the construction and use of a mental model (how does the user understand time?), and the user of an abstraction hierarchy (how much precision is required? Minutes only, but "twelve" is insufficient).

Another example, from the consultant working with an opera company:

> So, that's how that came about. And the way we tried to approach this problem was for one establishing with the client Seattle Opera Company in this example, establishing what kind of information they wanted do they want to give, what kind of donation levels they wanted to establish, and how can we create an interface that would give people the options to choose what they would like to fund and basically give that feedback going through the process of going through an online form to set up this funding cycles, so we approached it in – a couple of problems – how was the Seattle Opera Company, who don't really have technical teams to update this information – how would we have them update this information, create tiered funding, funding options without, you know, having to call up the interactive agency just to make simple text updates….And then basically take [the user] through the steps to making sure the process was linear so that he would understand that we started off with making the choice of – excuse me – the direction – the next step would be how much would they want to fund the donation and the third step was the actual financial information, so we had to create a linear kind of process so it was very simple for the user to go from step one, step two, step three without it being a confusing experience, especially because the demographics were some people who might be funding this kind of a cause or organization are likely to be in an older demographic it was opera-related – it tends to be an older demographic – so we had to kind of make it as simple as possible and not too many bells and whistles but at the same time sophisticated enough so that we could get information processed and user identified.

In this case, the designer defined the business goals of the design, then based the design decomposition on each business goal: funding levels, funding options, and user feedback necessary. Technical and user flow concerns were identified and managed in concert with each business goal, then broken down into a step-by-step user flow for further analysis and design iteration.

When it came to usable privacy and security problems, none of the participants talked through the decomposition of the usable privacy and security issue as seen above. Usable privacy and security issues were identified as individual concerns for a larger design, an example of a design problem that had already been de-composed. For example, from the speech user interface designer:

> When it comes to the security, the CCD code, well, you know, it's in different places on different cards. AmEx is on the front, VISA is on the back. Three digits on VISA, four digits on an AmEx, and at the time that we were developing this, on the back of a VISA it might not even be there at all. There might not even be a CCD code. They're ubiquitous, now, but at the time we were building this, you couldn't count on it being there….I clearly remember as coming up in usability studies were the difficulty of trying to figure out the most efficient way to get the security codes – CCD – from the caller, particularly given the possibility that it might not be there, so one of the first questions that we originally asked was, you know, something like AmEx is a lot easier because it's very consistent but if they selected VISA as their payment type, then we had a question of, you know, is there a three-digit code on the back of the card? And at the time, we had the grammar written just basically a yes/no grammar, you know, a yes and no and a number of variances on that, but again, you know, as soon as people started doing this, you know, it was like, you know, slapping myself on the forehead. I would say, look at that. Instead of saying yes or no, there would just be numbers. Well, that's because if they just said three numbers, that was as good as a "yes" and it saved a step. But the system would just say please say yes or no, so that was something that we had to fix across the iterations, so that the grammar instead of just being yes or no was also aware of the possibilities that somebody might simply speak three digits.

The usable privacy and security problem here was one of authentication. As part of the user flow, the designer needed to allow for the user to authenticate that they were holding the credit card they were using to pay. The authentication mechanism was the security code located on the back of the card. The usability challenge was in finding a straightforward and clear way of explaining to the user the location of the security code, and recognizing the code when the user gave it to the system.

It is worth repeating that the identified activity in this case was not "to authenticate the user." The activity was to allow the user to pay for items by phone. That challenge was, in turn, de-composed into the single design sub-task of authenticating via reading specific numbers off of a credit card.

This resonates with a point made by Egelman et al. [2007]: Security is not a primary task of the user. We can extend this into a logical but important observation: often, security is not a primary concern of the designer. Security and privacy are issues that designers need to contend with, but in de-composed fashion, not as primary tasks or goals.

We therefore see that except in the context of technical security issues, trust and privacy issues were often not successfully decomposed and modularized by the participants.

Synthesis

As this was an exploratory study, there were several framing questions to reflect upon in looking at the data from these interviews. Each of the interview participants had already identified themselves as a designer who worked on designs involving personally identifiable information (PII). How did these designers conceptualize security and privacy problems? Did the designers think of usability as an active part of the security and privacy discussion? Were there specific key points, either conceptual or process-driven, where usable privacy and security issues were considered in the context of the design process?

We have already seen how designers defined and decomposed their design problems, including security and privacy issues. One area that we have not yet explored, however, is that of *context*. As we have already seen, situated action and activity theory separately point out the need for designers to consider carefully the context of the action, not just the planned action and the goal.

How did the designers in this study conceptualize the context of use of their designs? Some designers considered context of use very carefully, others did not. Compare the designers who worked with mobile devices and voice interfaces, who were very concerned with the context of use and of the user, with the academic designer or the designer of the insurance system, who did not speak to issues of context of use. One could argue that there are two issues being conflated here. The first two designers were concerned with specific form factors, methods of input, where the other two designers in this

example largely avoided questions of form factor constraint. Is form factor the same as context? Not precisely. The form factor is an aspect of the context of use, but as we note from Nardi et al. [1996], activity theory suggests that the form factor is only one aspect. Others include the people with whom the user is working and interacting, the overall network of activities, and the setting in which the interaction takes place.

The academic designer offered a particularly interesting case in point. Unlike the other designers, the academic designer said nothing about how users would interact with his system, or about the context in which the system would be used. He did, however, make several points about the overall dynamic of the group that would use this particular system:

> I don't think the culture is quite there. It's susceptible to change, and this organization is just not a particularly chatty organization. The membership is pretty much moribund except for position announcements and calls for proposals periodically, and there are other organizations that I'm also on the mailing list that have much more eager actors within the membership.

In the domain of usable privacy and security, he offered additional insights:

> I tend to be fairly careful to document when announcing stuff to say to the membership, there's a million "ifs" but to say this is what we're doing. If you don't like it you should get in there and change your exposure to – you have to act, in the great existential dilemma, you have to act as something, and the next best thing to being guilty of mis-stepping is to, you know, act invisibly is worse, actually, so when we've done stuff that might potentially bother people in terms of privacy, is tell them about it.

Transparency to users is a key aspect of usable privacy and security, and one with which the designer was clearly familiar. As the population of users for the designer's system was relatively small and self-contained, the designer was able to be very direct with the communication, and to gauge the reaction that the users might have. The communication dynamic became a much more focused loop than is available for larger projects.

Recall Floridi's model of information ethics [Floridi 2006]. While none of the participants made specific reference to ethical concerns, the design problems they raised fell into one of two general categories. Some of the issues that they raised had to do with how a user completes a task or an activity. Most, however, dealt with, in various ways, integrity of data. The security and privacy concerns that each participant raised largely reflected data integrity: ensuring that data input was valid and authenticated, ensuring that systems could transmit data without threat of interception, and ensuring that data "at rest" - stored on a server - was not corrupted. These concerns fell primarily into Floridi's [2006] concerns about entropy: how to prevent and remove it from the infosphere, or at least the corner of the infosphere that fell into the designer's responsibility.

The implication of this finding is that, to varying degrees and in varying measure, the designers in this survey do have an awareness of and sensitivity to issues of privacy and security. Whether the designers were concerned with *usable* privacy and security is more difficult to discern. Certainly usability issues were mentioned in the course of the designers' discussions, but only two of the five designers - the speech UI designer and the bank designer - seemed heavily invested in the language, ideas and concepts of usability.

To summarize, therefore:

How did participants define the problem space and their audience? Participants conceptualized the problem space were around design constraints, iteration, and stakeholder input. Where usable privacy and security was mentioned in the conceptualization of the design, it was mentioned in the context of regulatory requirements rather than as a feature or concern in its own right.

Audience definition was, on the whole, considered a key aspect to the thinking and choices that went into the design. Audience definition was often a market segmentation exercise, thinking about marketing orientation.

How did the participants conceptualize trust? The findings here emphasized that trust issues are common issues in design. The nature of the design concerns around trust varied depending on the stakeholders' attitudes towards the actors and activities in question. For other participants, comments about trust were implicit and hard to tease out. For experienced designers, trust questions are not easily separated from other concerns in design.

How did the participants decompose and modularize problems of trust in their design thinking? On the whole, they did not. With the exception of technical security issues, where user interaction was less of a concern, trust and privacy issues were often not successfully decomposed and modularized by the participants.

In the final chapter, I will summarize these findings and point out some future directions for research.

Chapter 6: Conclusion

In the previous chapters we explored how the participants in this study responded to questions about the context of their work, their audience, and design problems relating to trust. In this chapter, I will further describe some of the themes that emerged from the analysis. I will also suggest some next steps and future lines of research.

Problem Space and Audience

To reiterate the first research question of this study: for the designers studied, how do they define their problem space and their audience? If the problem space is narrowly defined, do designers show more attention to privacy and security than if the problem space is broader?

We should return to Fogg's [2002] conception of "narrowly defined" problem spaces. In his book on "persuasive technology," one of the tools that Fogg recommends for persuasion is what he calls "reduction technology." Simplifying a complex task into a few clear steps reduces the "cost" of performing the task and makes the task more likely to be accomplished. Similarly, Fogg notes, persuasive design can be achieved by narrowly defining a design problem to include a specific definition of the task(s) to be accomplished and the expectations and social roles of an audience. The audience analysis allows for tailoring the design to a receptive audience, one that is interested in the benefit that the design brings.

In the survey and interview data, we saw that designers tended to conceptualize their audience in terms of market segments with certain common features. Users of an opera site were older, wealthy, and less computer-savvy. An important market segment for mobile phone banking was the under-served population who generally did not own computers and distrusted banks. The designer in the mobile

phone banking scenario was very deliberately and consciously seeking to convert a resistant audience to a receptive audience by tailoring the design to their needs and wishes. That effort was based on trust: allowing a previously distrustful audience to use an already-trusted interface for accomplishing their banking tasks. Trust is an implicit concept of the interaction design, but not necessarily limited to an explicit activity or task.

In the case of trust questions, we should remind ourselves that usable privacy and security issues in general, and trust questions in particular, are rarely if ever the primary task of a user. Instead, they are aspects of a broader task that the user sets out to achieve. With that in mind, how did the designers conceptualize the design problems that they saw, and integrate usable privacy and security into their conceptual model of those design problems?

We saw in the survey that 65.7% of the respondents reported that they had indeed worked on a design problem that required asking a trust question of a user. Put another way, nearly two thirds of the designers surveyed—who were, as a reminder, *not* selected from a pool of designers focused on privacy and security issues—had experience with designing trust questions for users. This is strongly suggestive that trust questions are indeed a common consideration in design.

We also saw through the interviews that, as with users, the designers I interviewed often did not conceptualize their design problems as trust questions, or even more broadly as privacy and security problems. Instead, the privacy and security issues were wrapped up in larger design concerns: adapting existing banking scenarios to a mobile device context, or adapting a membership system to new technology, or upgrading a site for an opera company. See Chapter 5 for specific examples of these conceptions.

Many of the reported conceptualization of design problems followed Fogg's [2002] ideas of a "narrowly focused" design problem: the audience was known and understood (e.g. opera lovers: primarily wealthy, primarily older, not expected to be very technology savvy) and the persuasive tasks

were simple and well defined (persuade the opera lovers to sign up to donate to the local opera company.) That these tasks involved a trust question ("do I trust the opera company with my credit card?") was an implicit assumption but not explicitly stated or conceptualized as a design problem. If the trust question had been explicitly stated or conceptualized, the participants would have invoked a trust concept explicitly. They did not do so.

How did the designers conceive of the problem? As we have seen, the problem space defined by the designers generally fell into the following categories:

Audience

Stakeholder concerns & business strategy

Technical challenges

Authentication & access, encryption

Another way to frame the notion of the technical challenges is in notion of technical *constraints*: constraints of practicality or engineering. Design must often adapt to what can be built using the existing technology and code available to the designer. Many of the challenges mentioned in both survey and interviews fell into this category. This was expected; the design literature is full of studies on how designers work within particular technical constraints (see [Jones 1992] for an example). From the point of view of the usable privacy and security literature, issues of authentication and access as well as encryption often fell into the same category. A challenge in creating a voice-based authentication scheme using a credit card is essentially a challenge of designing for constraints. The credit card has only certain information. Voice can only transmit certain kinds of information. The design challenge becomes in creating a scheme that will work within those given constraints.

With all of that in mind, there were intriguing counter-examples. In Chapter 4, we saw the example of the respondent who was deeply versed in privacy issues around location awareness:

> Figuring out how to inform the user about the fact that their location was being used in a short time frame over the voice channel (on a phone call) as well as determining how exactly to use the location, especially given that we had varying degrees of accuracy, was particularly challenging.

Consider also this quote from a survey respondent:

> Making clear the distinction between what personalized data you're collecting that remains private vs. public can be difficult. Particularly if users have the option of getting more specific than the defaults in what they do/don't share.

This is a "pure" trust question problem, in the sense that it has nothing to do with the overall task that the user is trying to achieve. Instead, said the designer, the problem was in "making clear the distinction" for the relative privacy levels of collected data. In most cases, the need to make clear that distinction is driven strictly by the privacy needs we examined earlier. Of the dozens of design problem descriptions I collected, these were the only two instances where the designer clearly conceptualized a design problem *as* a usable privacy and security problem.

Both the survey and the interview protocols were designed to avoid the use of the word *trust* and to avoid concentrating exclusively on usable privacy and security issues. It is possible—even likely—that with prompting the participants might have engaged in further conceptualization of usable privacy and security problems in their work. The data shows that the participants were aware of privacy and security as domains of interest.

This analysis, however, must be judged in light of prior attitudinal research in the usable privacy and security field. Repeated studies have shown in many contexts that users faced with privacy and security problems will claim that they follow best practices not actually seen in behavioral studies [Dourish and Anderson 2006; Goldman and Christie 2004; Sotirakopoulos, Hawkey and Beznosov 2011].

One of the key principles in the design of this study was to avoid, to the extent possible, prompting the participants to think more deeply about privacy and security than they would under natural

circumstances. It is significant that without the extra prompting, the participants showed a lack of usable privacy and security conceptualization.

It is important not to overstate the case, however. While the survey and interview did not oversell the issue, both included questions that were directly related to usable privacy and security and gave ample opportunity for the participants to reflect on their experiences with the domain. As we have seen, two participants did so.

Another example that cropped up in the survey and interview data more than once is the tension between business requirements, the amount of data that users were willing to share, and the potential uses for that data. "The business [wanted] to work in additional cross sell opportunities," wrote one respondent. The designer is forced to mediate between conflicting requirements in determining exactly how to collect the data and how much data to collect. An interesting area of future research would be determining which of the conflicting requirements tended to win.

We saw in Chapter 5 the example of the designer who somewhat casually mixed the notions of data use for transactional and marketing purposes. Data collection, use and reuse is a carefully modularized problem space for privacy advocates, but here was an example of a designer who conflated several aspects of data use together. The implication is that the working designers in this survey do not decompose or modularize usable privacy and security problems in the same way that advocates do.

In the next section, we will look further at these notions of de-composition and modularization.

Decomposition and Modularity

Goel & Pirolli [1992], in their discussion of the structure of design problems, talk about two important concepts already mentioned at length: modularity and decomposability. In their words:

Given the size and complexity of design problems and the limited capacity of short-term memory, one would expect decomposition of the problem into a large number of modules. However, given the fact that there are few or no logical connections among modules but only contingent ones, one would expect the designer to attend to some of these and ignore the others.

With some notable exceptions the designers in this study tended to integrate usable privacy and security problems in general—and trust questions in particular—with larger problems of design. Designers in this study did not report treating usable privacy and security as a separate, modularized design concern. Instead, the problem was tightly integrated with other aspects of the design that the designers are seeing. We have already seen the example of the speech user designer. Other examples included the designer for the insurance company, who saw their design as an intersection between architectural and business and regulatory requirements, and the designer who looked at the problems of identity in a cloud environment.

One designer summarized the problem of integration in terms of the roles of the people working on it:

> This is probably not an uncommon challenge; the technologists have a habit of thinking only of the system and the gracefulness of the technical solution, and not necessarily how that is impacting the user. So, one of the things that I needed to do along with the designer from the business application was remind the architect and the people doing services that we needed to provide sufficient details about the data that they couldn't see to get them in the security so that the data was actually there, in fact.

It is important to be clear that the designers are decomposing and creating modularity in their design problems. We see many instances of the decomposition process throughout the data set, as the designers

talked through their process. The designer for an insurance company in particular walked through a detailed, step-by-step decomposition of her design problem, beginning with the user scenario, talking through each relevant system and their connections, and ending with the issues surrounding the use of debit cards in her scenarios. However, the instances where designers in this study decomposed and created modularization of their *usable privacy and security* problems were few in number. Given that usable privacy and security problems are demonstrated to be common among the designers surveyed, this is a surprising finding based on my hypothesis.

To belabor an important point, modularization of *security* problems — encryption, for example — is commonplace. *Usable privacy and security* encompasses a larger set of concerns including ethical issues of trust, usability, and relationship management separate from issues of authentication and authorization. It is the modularization of usable privacy and security that was not apparent in the data.

What are the implications of this lack of decomposition & modularization? Because the designers in this study did not, on the whole, create modularity in their usable privacy and security problems, they did not demonstrate the ability to decompose privacy issues to their component parts and apply a structured approach to resolving the problem.

Consider, again, the example of the designer who nearly conflated the use of data for marketing with the use of data to accomplish a transaction:

> There wasn't really data mining going on, we weren't being Facebook about this. It was purely just so they could process the financial transactions. There wasn't anything other than that. Also so they could send out marketing, which we had opt-in options for.

Information given to complete a financial transaction is not the same as information given for opt-in marketing purposes, but this designer did not clearly differentiate between the two. The potential for creating potential privacy issues and lack of trust when these two elements are conflated is quite high.

Another example from the survey data was this participant's report:

> Main design problem was updating the customer's personal information when the actual customer present was their spouse. We needed to store the updates, but could not validate them until the actual spouse was present.

This was survey data, not interview data, so it was impossible to follow up with a probing question. It may be that the participant had a more nuanced view of the problem that could not be delivered in a short answer. Taken at face value, however, this response suggests that they have conflated several issues: the task (updating personal information), with authentication (checking their spouse's ID) and verification (validating that the primary information owner meant to update the information). The trust issues are on the part of both the participant's organization ("are you who you say you are and are you representing the request accurately?") and on the user ("will the organization protect me from having my personal information maliciously or erroneously changed?") The suggestion that the primary information owner had to be physically present to make information updates indicates that there was a high degree of risk associated with the potential loss of information, but the exact risks remain unstated.

Trust Questions

Finally, the study asked: How do designers conceptualize the problem of trust questions in relation to the overall design space in which they are engaged? In what contextual relationship and framing do they place trust questions?

We have already seen that trust questions are a common design problem and that trust questions are rarely conceptualized as such by the designers in this data set. We also saw that trust was a common concern of designers in a number of different scenarios. These included:

User emotion. In both the survey data and interview data, there was evidence that designers sought to use persuasive design to encourage users past negative emotions toward an organization or system. Examples included the audience being encouraged to use mobile banking software and the audience

seeking help with a credit report. One designer reported working to overcome "fear and ingrained behavior" in an audience, while another wrote of designing "so that trust was ensured."

Identity and sharing. Many designers reported that authenticating an identity was a major concern both from a security and a trust perspective. (Recall that systems need to authenticate users in order to "trust" that the user is accessing the correct information.) We saw one example from the survey data that probed deeply into the notion of public versus private identity in a data-sharing scenario in cloud storage.

Ethics. In both the survey and interview data, we saw designers wrestling with the question of "doing the right thing," — not just a technically viable, usable solution, but a solution that would best suit the interests of users and stakeholders alike. Consider the example of the designer looking at GPS data: the question was not about whether the GPS data could be stored, but whether the user would want to do so, or even if it was a concept they would understand. Privacy requirements and regulation played a role in this decision. It also appeared, however, that the ethical considerations of storing location data without the user's full understanding of the implications—even with their consent secured—was equally important.

We therefore can say with confidence that issues of trust are understood among at least a subset of the designers surveyed. It is worth the reminder, however, that many of the designers in the survey and the interviews did not appear to decompose or modularize trust issues in their own work. Trust issues, issues of privacy and security, may be an area of awareness for the designer, but the designer may not be able to tease those issues out from the overall concerns of the design problem.

This resonates with a finding about user perceptions of privacy, mentioned earlier in Chapter 2: the privacy paradox. User behavior often does not match user expression of privacy concern. Users who express concern about their privacy online will give up that privacy in exchange for a service perceived to

be useful. Similarly, it may be that designers will be able to speak to issues of privacy and trust without being able to decompose their own design problems into their trust issues.

Recall also that the work of Helen Nissenbaum [2004] and her collaborators helped establish that information privacy - from which trust is often derived—is not a "feature" that can be written for a system, but a mindset and analysis that must be brought to bear through the user experience design process. Bearing this in mind, is it possible for designers to create trust without the necessary decomposition and modularity that a more explicit design problem structuring [Cross 2001; Goel and Pirolli 1992; Petre 2009] would establish?

Future Work

I have called this an exploratory study. I believe this charts new territory for potential research in usable privacy and security. What are the next logical directions for this research?

Riegelsberger et al. [Riegelsberger et al. 2003; Riegelsberger and Vasalou 2007] noted four areas of study of trust: objects of trust and related risk, methods and background of trust, models and frameworks of trust, and goals of trust research.

This study was intended to address the methods and background of trust through interrogating the process of creating trust questions from the designer's point of view. The findings helped to point out that the existing models and frameworks of trust, while helpful, may not directly relate to the working experience of designers not embedded in the usable privacy and security discourse community. Without a consistent model for decomposing and modularizing trust problems for working designers, we risk a false understanding in the usable privacy and security field of how to help designers create more trust through their own designs.

This suggests two logical lines of research for the future. First, the usable privacy and security discourse community should look at how to help designers with that modularization and decomposition

process. Using Riegelsberger's model [Riegelsberger and Vasalou 2007], this would likely be a study of objects of trust as well as the models and frameworks of trust: finding a model that aligns closely with how designers are conceptualizing their own design problems

Second, the usable privacy and security discourse community should continue to look more deeply at the practice of design as it relates to usable privacy and security problems. This dissertation has underscored how hard the phenomenon of usable privacy and security is to pin down. Condensed contextual inquiry [Kantner et al. 2003], in depth interviews, and other qualitative methods may help to shine light on the points where usable privacy and security modeling and guidance can be of best input to working designers, and can provide real world solutions to problems that are well established in the literature as serious and pervasive in the modern information space.

Future Implications for Practice

Usable privacy and security is not just a theoretical field but a practical one as well. Usable privacy and security studies are often directed towards providing prescriptive advice or assistance to working designers, whether in the form of user interface models, design patterns, or usability studies. With that knowledge in mind, we should ask ourselves: can the work here inform the practice of usable privacy and security design?

To repeat myself for a moment, one of this study's most important findings is that the working designers who participated do not decompose or modularize usable privacy and security problems in the same way that advocates for usable privacy and security do. The implication for practice here is that attempts to force that level of modularization on designers—for example, through the use of a design pattern strictly intended as a privacy solution—may not be as effective. Instead, research outcomes intended for practical use should look for ways to integrate strong usable privacy and security practices with other, related design problems. A design pattern for an icon or browser toolbar, for example, may be

less effective than a design pattern for an integrated "checkout" experience that incorporates usable privacy and security research. To ask again a question from chapter 5: Is it possible that emphasizing quality audience analysis research and practices would improve our understanding of how to positively influence design for usable privacy and security?

We have also verified that trust questions are decision points of trust, and as such are a key focal point of usable privacy and security design. The implication for practice is that, because of the issues with modularity, trust questions may not be directly perceived as trust decisions *even by the designer*. Therefore, the usable privacy and security discourse community should not rely on the language of trust decisions to persuade designers to good practice, but rather on identifying and improving the design practice for the decision point as a whole, with trust, usability, aesthetics, effectiveness, and all other implications accepted in a holistic and encompassing way.

Conclusion

The study of the designer's approach to usable privacy and security problems is a new and fascinating space of inquiry. My initial explorations of this space have shown that usable privacy and security problems are common for working designers, and raised a key question. Many designers working on usable privacy and security issues do not see the modularity that usable privacy and security researchers implicitly assume in much of their research and guidance. Without that modularity, members of the usable privacy and security discourse community face the risk of false understanding.

The contributions of this study are as follows. I have shown how designers conceptualize the problem space of usable privacy and security. I have shown that decomposition and modularity remain difficult for designers in the context of trust and usable privacy and security problems. Finally, I have shown that trust questions are both a common problem for designers and a key potential point for improved design practice.

Privacy and security is not exclusively a technology-based problem that can be fixed with code or a single feature or even a full business architecture. Privacy and security lead to trust, and trust is about human behavior. It is understood in the design community as well as the usable privacy and security community that to promote trust, the human reaction to an interface must be carefully understood. To date it has been less common to think of the human behavior *of the designer* in grappling with trust questions and other usable privacy and security problems. I hope this study points the way to future investigation of this important topic.

References

Ackerman, Mark S., and Scott D. Mainwaring. "Privacy Issues and Human-Computer Interaction." In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorie Faith Cranor and Simson Garfinkle, 381-400. Sebastopol, CA: O'Reilly, 2005.

Adams, Anne, and M. Angela Sasse. "Users Are Not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures." *Communications of the ACM* 42, no. 12 (December 1999 1999).

Al Zomai, Mohammed, Bander Al Fayyadh, Audun Jøsang, and Adrian McCullagh. "An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems." Paper presented at the Sixth Australasian Conference on Information Security, Wollongong, NSW, Australia, 2008.

Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley Computer Publishing, 2001.

Baldwin, Carliss Young, and Kim B Clark. *Design Rules: The Power of Modularity*. Vol. 1: mIt Press, 2000.

Barth, Adam, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. "Privacy and Contextual Integrity: Framework and Applications." Paper presented at the IEEE Symposium on Security and Privacy, Oakland, CA, 2006.

Beautement, Adam, and AM Sasse. "Gathering Realistic Authentication Performance Data through Field Trials." Paper presented at the SOUPS USER Workshop, 2010.

Beyer, H., and K. Holtzblatt. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann Pub, 1998.

Beyer, Hugh, and Karen Holtzblatt. *Contextual Design: Defining Customer-Centered Systems*. San Francisco, CA: Morgan Kaufmann, 1998.

Biernacki, Patrick, and Dan Waldorf. "Snowball Sampling: Problems and Techniques of Chain Referral Sampling." *Sociological Methods & Research* 10, no. 2 (1981): 141-63.

Birks, Melanie, and Jane Mills. *Grounded Theory: A Practical Guide*. Los Angeles: Sage, 2011.

Boczkowski, Pablo J. "Mutual Shaping of Uses and Technologies in a National Virtual Community.". *Journal of Communication* 49 (1999): 86-108.

boyd, danah. "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence." *Convergence: The International Journal of Research into New Media Technologies* 14, no. 1 (2008): 13-20.

Burnard, Philip. "A Method of Analysing Interview Transcripts in Qualitative Research." *Nurse Education Today* 11, no. 6 (12// 1991): 461-66.

Firesheep. Codebutler.com.

Carrow, Erwin Louis. "Puppetnets and Botnets: Information Technology Vulnerability Exploits That Threaten Basic Internet Use." Paper presented at the Proceedings of the 4th annual conference on Information security curriculum development Kennesaw, GA, 2007.

Castells, M. *The Rise of the Network Society (2nd Ed.)*. Vol. 1, Oxford, UK: Blackwell, 2000.

Charmaz, Kathy, and L Belgrave. "Qualitative Interviewing and Grounded Theory Analysis." *Sage, Thousand Oaks, CA* (2003): 311-30.

Chiasson, Sonia, R. Biddle, and P C van Oorschot. "A Second Look at the Usability of Click-Based Graphical Passwords." Paper presented at the ACM Symposium on Usable Securty and Privacy (SOUPS 2007), Pittsburgh, PA, 2007.

Chopra, Samir, and Laurence White. "Privacy and Artificial Agents, or, Is Google Reading My Email?" Paper presented at the Proceedings of the 20th international joint conference on Artifical intelligence, 2007.

Clark, David D. "End-to-End Argument and Application Design: The Role of Trust, The." *Fed. Comm. LJ* 63 (2010): 357.

Cofta, Piotr. *Trust, Complexity and Control: Confidence in a Convergent World*. 2007.

Condon, Christopher, and Scott Morrison. "Phishing, Pharming and Fraud: How Hacker's Prying Eyes Threaten Confidence in Online Commerce.". *Financial Times* (March 9, 2005 2005 (Mar 9)): 17.

Cranor, Lorie Faith. *Web Privacy with P3p*. Sebastopol, CA: O'Reilly, 2002.

———. "What Do They "Indicate?": Evaluating Security and Privacy Indicators." *Interactions* 13, no. 3 (May + June 2006 2005): 45-47.

Cranor, Lorie Faith, and Simson Garfinkle. "Preface." In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorie Faith Cranor and Simson Garfinkle, ix-xvii. Sebastopol, CA: O'Reilly, 2005.

Cross, N. "Expertise in Design: An Overview.". *Design Studies* 25, no. 5 (2004): 427-41.

Cross, Nigel. "Designerly Ways of Knowing: Design Discipline Versus Design Science." *Design issues* 17, no. 3 (2001): 49-55.

"Cve-2003-0533." Department of Homeland Security, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533.

de Carvalho, Diego F., Rafael Chies, André P. Freire, Luciana A. F. Martimiano, and R. Goularte. "Video Steganography for Confidential Documents: Integrity, Privacy and Version Control." In *SIGDOC '08: 26th annual ACM international conference on Design of communication*, 199-206. Lisbon, Portugal: ACM Press, 2008.

de Paula, Rogério, Xianghua Ding, Paul Dourish, Kari Nies, Ben Pillet, David Redmiles, Jie Ren, Jennifer Rode, and Roberto Silva Filho. "Two Experiences Designing for Effective Security." Paper presented at the Proceedings of the 2005 Symposium on Usable Privacy and Security, Pittsburgh, PA, 2005.

Dillman, Don A. *Mail and Internet Surveys: The Tailored Design Method--2007 Update with New Internet, Visual, and Mixed-Mode Guide*. Wiley, 2011.

Dorst, K. "Viewpoint: Design Research: A Revolution Waiting to Happen.". *Design Studies* 29, no. 1 (2008): 4-11.

Dourish, P, and K Anderson. "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena." *Human Computer Interaction* 21, no. 3 (2006): 319-42.

Dumas, Joseph, and Janice Redish. "Introducing Usability Testing, Selecting and Organizing Tasks to Test, and Creating Task Scenarios." In *A Practical Guide to Usability Testing, Second Edition*, 21-38, 159-82. Portland, OR: Intellect, 1999.

"Ec-Council: Certified Ethical Hacker." https://www.eccouncil.org/certification/certified_ethical_hacker.aspx.

Egelman, S., J. Tsai, L.F. Cranor, and A. Acquisti. "Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators." 2009.

Egelman, Serge, Lorie Faith Cranor, and Jason Hong. "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings." Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08), Florence, Italy, 2008.

Egelman, Serge, Jennifer King, Robert C. Miller, Nick Ragouzis, and Erika Shehan. "Security User Studies: Methodologies and Best Practices." Paper presented at the CHI '07 extended abstracts on Human factors in computing systems, San Jose, CA, USA, 2007.

Engeström, Yrjo. "Activity Theory and Individual and Social Transformation." In *Perspectives on Activity Theory*, edited by Yrjo Engeström, R. Miettinen and R.L. Punamaki. Cambridge, MA: Cambridge University Press, 1999.

Farnham, Shelly D., and Elizabeth F. Churchill. "Faceted Identity, Faceted Lives: Social and Technical Issues with Being Yourself Online." In *Proceedings of the ACM 2011 conference on Computer supported cooperative work*, 359-68. Hangzhou, China: ACM, 2011.

Flechais, I., and M.A. Sasse. "Stakeholder Involvement, Motivation, Responsibility, Communication: How to Design Usable Security in E-Science." *International Journal of Human-Computer Studies* 67, no. 4 (2009): 281-96.

Floridi, Luciano. "Information Ethics, Its Nature and Scope." *ACM SIGCAS Computers and Society* 36, no. 3 (2006): 21-36.

Fogg, B J. *Persuasive Technology: Using Computers to Change What We Think and Do*. San Francisco, CA: Morgan Kaufmann, 2002.

Friedberg, Jeffrey. "End to End Trust and the Trust User Experience." http://blogs.technet.com/privacyimperative/archive/2009/04/24/end-to-end-trust-and-the-trust-user-experience.aspx.

Friedman, Batya. "Value-Sensitive Design." *Interactions* 3, no. 6 (1996): 16-23.

———. "The Watcher and the Watched: Social Judgements About Privacy in a Public Place." *Human Computer Interaction* 21, no. 2 (2006): 235-72.

Friedman, Batya, David Hurley, Daniel C. Howe, Edward W. Felten, and Helen Nissenbaum. "Users' Conceptions of Web Security: A Comparative Study." Paper presented at the Conference on Human Factors in Computing Systems (CHI '02), Minneapolis, MN, 2002.

Friedman, Batya, Peyina Lin, and Jessica K. Miller. "Informed Consent by Design." In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorie Faith Cranor and Simson Garfinkle, 495-522. Sebastopol, CA: O'Reilly, 2005.

Gaver, William. "Technology Affordances." Paper presented at the Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '91), New Orleans, LA, 1991.

Gaw, S., E.W. Felten, and P. Fernandez-Kelly. "Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email." 2006.

Gefen, David. "Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers." *ACM SIGMIS Database* 33, no. 3 (2002): 38-53.

Gilman, Michele E. "The Class Differential in Privacy Law." *Brooklyn Law Review* 77, no. 4 (2012).

Glaser, Barney G., and Anselm L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company, 1967.

Goel, V., and P. Pirolli. "The Structure of Design Problems and Spaces.". *Cognitive Science* 16, no. 3 (1992): 395-429.

Goldman, James E., and Vaughn R. Christie. "Metrics Based Security Assessment." In *Information Security & Ethics: Social and Organizational Issues*, edited by Marian Quigley, 261-88. Hershey, PA: IRM Press, 2004.

Goles, Tim, Gregory B. White, Nicole Beebe, Carlos A. Dorantes, and Barbara Hewitt. "Moral Intensity and Ethical Decision-Making: A Contextual Extension." *SIGMIS Database* 37, no. 2-3 (2006): 86-95.

Gomila, Toni, and Paco Calvo. "Directions for an Embodied Cognitive Science: Toward an Integrated Approach." *Handbook of cognitive science: An embodied approach* (2008): 1-25.

Greenberg, Saul, and Bill Buxton. "Usability Evaluation Considered Harmful (Some of the Time)." Paper presented at the Conference on Human Factors in Computing Systems (CHI 2008), Florence, Italy, 2008.

Hansche, Susan, John Berti, and Chris Hare. *Official Isc(2) Guide to the Cissp Exam*. Boca Raton, FL: Auerbach Publications, 2004.

Hoffman, R.R., and G. Lintern. "Eliciting and Representing the Knowledge of Experts." *Cambridge handbook of expertise and expert performance* (2006): 203ñ22.

Hoffman, Robert R., Beth Crandall, and Nigel Shadbolt. "Use of the Critical Decision Method to Elicit Expert Knowledge: A Case Study in the Methodology." [In English]. *Human Factors* 40, no. 2 (1998).

Hogg, Michael A., and Deborah J. Terry. "Social Identity and Self-Categorization Processes in Organizational Contexts." *The Academy of Management Review* 25, no. 1 (2000): 121-40.

Hogg, Michael A., Deborah J. Terry, and Katherine M. White. "A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory." *Social Psychology Quarterly* 58, no. 4 (1995): 255-69.

Hughes, Michael. "Rigor in Usability Testing." *Technical Communication* 46, no. 4 (1999): 488-94.

Iachello, Giovanni, Ian Smith, Sunny Consolvo, Mike Chen, and Gregory D. Abowd. "Developing Privacy Guidelines for Social Location Disclosure Applications and Services." Paper presented at the Proceedings of the 2005 symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2005.

Jaferian, P., K. Hawkey, A. Sotirakopoulos, and K. Beznosov. "Heuristics for Evaluating It Security Management Tools." 2011.

Johnson, Robert R. *User-Centered Technology: A Rhetorical Theory for Computers and Other Mundane Artifacts*. Albany, NY: State University of New York Press, 1998.

Johnston, J., J.H.P. Eloff, and L. Labuschagne. "Security and Human Computer Interfaces." *Computers & Security* 22, no. 8 (2003): 675-84.

Jones, John Chris. *Design Methods*. John Wiley & Sons, 1992.

Kantner, Laurie, Deborah Hinderer Sova, and Stephanie Rosenbaum. "Alternative Methods for Field Usability Research." Paper presented at the Proceedings of the 21st annual international conference on Documentation, 2003.

Kaptelinin, Victor, and Bonnie Nardi. *Acting with Technology: Activity Theory and Interaction Design*. Cambridge, MA: MIT Press, 2006.

Kaptelinin, Victor, Bonnie Nardi, Suzanne Bødker, John Carroll, Jim Hollan, Edwin Hutchins, and Terry Winograd. "Post-Cognitivist Hci: Second-Wave Theories." In *CHI '03 extended abstracts on Human factors in computing systems*. Ft. Lauderdale, Florida, USA: ACM, 2003.

Kayacik, H.G., and A.N. Zincir-Heywood. "Mimicry Attacks Demystified: What Can Attackers Do to Avoid Detection?" Paper presented at the Sixth Annual Conference on Privacy, Security and Trust (PST '08), Fredericton, New Brunswick, Canada, 2008.

Kikkawa, T., S. Shirato, S. Fujiiand, and K. Takemura. "The Pursuit of Informed Reassurance ('an-Shin'in Society) and Technological Safety ('an-Zen')." *Journal of SHAKAI-GIJUTSU* 1 (2003): 1-8.

Kim, Jun H., Daniel V. Gunn, Eric Schuh, Bruce Phillips, Randy J. Pagulayan, and Dennis Wixon. "Tracking Real-Time User Experience (True): A Comprehensive Instrumentation Solution for Complex Systems." Paper presented at the Conference on Human Factors in Computing Systems (CHI '08), Florence, Italy, 2008.

Kitzinger, Celia. "After Post-Cognitivism." *Discourse Studies* 8, no. 1 (2006): 67-83.

Klasnja, P., S. Consolvo, J. Jung, B.M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall. "When I Am on Wi-Fi, I Am Fearless: Privacy Concerns & Practices in Everyday Wi-Fi Use." 2009.

Klein, Gary A, Roberta Calderwood, and Donald MacGregor. "Critical Decision Method for Eliciting Knowledge." *IEEE Transactions on Systems, Man, and Cybernetics* 19, no. 3 (1989): 462-72.

Kline, Ronald, and Trevor Pinch. "Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States.". *Technology and Culture* 37, no. 4 (1996): 763-95.

Krumaraguru, P., and Lorie Faith Cranor. "Privacy Indexes: A Survey of Westin's Studies." Carnegie Mellon University, http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

Kuutti, Kari. "Activity Theory as a Potential Framework for Human-Computer Interaction Research." *Context and consciousness: Activity theory and human-computer interaction* (1996): 17-44.

Langlois, Richard. "Modularity in Technology, Organization, and Society." *Organization, and Society (August 1999)* (2000).

Lessig, Lawrence. "Prosecutor as Bully." 2013.

Levy, Steven. *Hackers: Heroes of the Computer Revolution*. Penguin, 2001.

Li, Na, Maryam Najafian Razavi, and Denis Gillet. "Trust-Aware Privacy Control for Social Media." Paper presented at the Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems, 2011.

Lieberman, Evan S. "Nested Analysis as a Mixed-Method Strategy for Comparative Research." *American Political Science Review* 99, no. 03 (2005): 435-52.

Lindgaard, G., and C. Dudek. "What Is This Evasive Beast We Call User Satisfaction?". *Interacting with computers* 15, no. 3 (2003): 429-52.

MacKenzie, I Scott. "Fitts' Law as a Research and Design Tool in Human-Computer Interaction." *Human-computer interaction* 7, no. 1 (1992): 91-139.

Miller, Carolyn R. "Expertise and Agency: Transformations of Ethos in Human-Computer Interaction." In *The Ethos of Rhetoric*, edited by Michael J Hyde. Columbia, SC: University of South Carolina Press, 2004.

Mills, Jane, Ann Bonner, and Karen Francis. "The Development of Constructivist Grounded Theory.". *International Journal of Qualitative Methods* 5, no. 1 (2006).

Mohr, Jakki, Sanjit Sengupta, and Stanley Slater. *Marketing of High-Technology Products and Innovations*. 2nd ed. New Jersey: Pearson Prentice Hall, 2005.

Moorman, Robert H, and Philip M Podsakoff. "A Meta-Analytic Review and Empirical Test of the Potential Confounding Effects of Social Desirability Response Sets in Organizational Behaviour Research." *Journal of Occupational and Organizational Psychology* 65, no. 2 (1992): 131-49.

Mosborg, Susan, Robin Adams, Rebecca Kim, Cynthia J Atman, Jennifer Turns, and Monica Cardella. "Conceptions of the Engineering Design Process: An Expert Study of Advanced Practicing Professionals." Paper presented at the Proceedings of the 2005 American society for engineering education annual conference & exposition, 2005.

Muñoz-Arteaga, Jaime, Ricardo Mendoza González, Miguel Vargas Martin, Jean Vanderdonckt, and Francisco Álvarez-Rodriguez. "A Methodology for Designing Information Security Feedback Based on User Interface Patterns.". *Advances in Engineering Software*, no. in press (2009).

Murayama, Y., C. Hauser, Y. Fujihara, D. Nishioka, and A. Inoue. "The Comparison Study between the Us and Japan on the Sense of Security, Anshin, with Non-Computer-Science Students." 2011.

Murayama, Y., N. Hikage, Y. Fujihara, and C. Hauser. "The Structure of the Sense of Security, Anshin." *Critical Information Infrastructures Security* (2008): 83-93.

Nardi, B.A. "Studying Context: A Comparison of Activity Theory, Situated Action Models, and Distributed Cognition." *Context and consciousness: Activity theory and human-computer interaction* (1996): 69-102.

Nardi, Bonnie. *Context and Consciousness: Activity Theory and Human-Computer Interaction*. Cambridge, MA: MIT Press, 1996.

Nathan, Lisa P, and Alex Garnett. "Privacy Research & "Real World" Design: Is There an Elephant in the Room?". (

Newell, A., and S.K. Card. "The Prospects for Psychological Science in Human-Computer Interaction." *Human Computer Interaction* 1, no. 3 (1985): 209-42.

Nielsen, J. "Usability Testing." In *Usability Engineering*, 165-206. San Francisco: Morgan Kaufmann, 1993.

Nissenbaum, H. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17, no. 5 (1998): 559-96.

Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* 79, no. 1 (2004): 119-58.

———. "Will Security Enhance Trust Online, or Supplant It?". In *Trust and Distrust within Organizations: Emerging Perspectives, Enduring Questions*, edited by R. Kramer and K. Cook, 155-88. New York: Russell Sage Publications, 2004.

Nodder, Chris. "Users and Trust: A Microsoft Case Study." In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorie Faith Cranor and Simson Garfinkle, 589-606. Sebastopol, CA: O'Reilly, 2005.

Norman, Don. "Logic Versus Usage: The Case for Activity-Centered Design.". *Interactions* 13, no. 6 (2006): 45-63.

———. *The Psychology of Everyday Things.* New York: Basic Books, 1988.

Norman, Don, and S W Draper. *User-Centered System Design: New Perspectives on Human-Computer Interaction*. Hillsdale, NJ: Lawrence Erlbaum, 1986.

Norman, Donald. "Cognitive Artifacts." In *Designing Interaction: Psychology at the Human-Computer Interface*, edited by John Carroll, 17-38: Cambridge University Press, 1991.

Norman, Donald A. *Emotional Design: Why We Love (or Hate) Everyday Things*. Basic books, 2003.

Oetzel, Marie Caroline, and Tijana Gonja. "The Online Privacy Paradox: A Social Representations Perspective." Paper presented at the Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems, 2011.

Ong, Walter. "The Writer's Audience Is Always a Fiction." *Publication of the Modern Language Association* 90 (1975): 9-21.

Parkin, Simon, Aad van Moorsel, Philip Inglesant, and M Angela Sasse. "A Stealth Approach to Usable Security: Helping It Security Managers to Identify Workable Security Solutions." Paper presented at the Proceedings of the 2010 workshop on New security paradigms, 2010.

Patrick, Andrew S., Pamela Briggs, and Stephen Marsh. "Designing Systems That People Will Trust." In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorie Faith Cranor and Simson Garfinkle, 75-100. Sebastopol, CA: O'Reilly, 2005.

Petre, M. "Insights from Expert Software Design Practice." 2009.

Pinch, Trevor, and Wiebe Bijker. "The Social Construction of Facts and Artifacts, or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other.". In *The Social Construction of Technological Systems*, edited by Wiebe Bijker, Thomas P. Hughes and Trevor Pinch, 17-50. Cambridge, MA: MIT Press, 1987.

Pollach, Irene. "What's Wrong with Online Privacy Policies?". *Communications of the ACM* 50, no. 9 (2007): 103-08.

"Privacy Guidelines for Developing Software Products and Services." (2010). Published electronically 9/29/2010. http://www.microsoft.com/en-us/download/details.aspx?id=16048.

Putnam, Cynthia. "Bridging the Gap between User Experience Research and Design in Industry: An Analysis of Two Common Communication Tools--Personas and Scenarios." University of Washington, 2010.

Radics, Peter J, and Denis Gracanin. "Privacy in Domestic Environments." Paper presented at the Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems, 2011.

Raymond, Eric S. "Jargon File: Hacker." http://www.catb.org/jargon/html/H/hacker.html.

Riegelsberger, J., M.A. Sasse, and J.D. McCarthy. "The Mechanics of Trust: A Framework for Research and Design." *International Journal of Human-Computer Studies* 62, no. 3 (2005): 381-422.

Riegelsberger, Jens M, M Angela Sasse, and John D McCarthy. "The Researcher's Dilemma: Evaluating Trust in Computer-Mediated Communication." *International Journal of Human-Computer Studies* 58 (2003): 759-81.

Riegelsberger, Jens M., and Asimina Vasalou. "Trust 2.1: Advancing the Trust Debate." Paper presented at the CHI '07 extended abstracts on Human factors in computing systems, San Jose, CA, USA, 2007.

Rotter, J.B. "A New Scale for the Measurement of Interpersonal Trust1." *Journal of personality* 35, no. 4 (1967): 651-65.

Saltzer, Jerome, and Michael Schroeder. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63, no. 9 (1975): 1278-308.

"Sasser Creator Avoids Jail Term." BBC News, http://news.bbc.co.uk/2/hi/technology/4659329.stm.

Sasso, Brendan, and Jennifer Martinez. "Lawmakers Slam Doj Prosecution of Swartz as 'Ridiculous, Absurd'." In *Hillicon Valley*, 2013.

Shalloway, Alan, and James Trott. *Design Patterns Explained: A New Perspective on Object-Oriented Design*. Addison-Wesley Professional, 2005.

Sharmila Deva Selvi, S., S. Sree Vivkek, N.N. Karuturi, R. Gopalakrishnan, and P.R. Chandrasekaran. "Cryptanalysis of Bohio Et Al.'S Id-Based Broadcast Signcryption (Ibbcs) Scheme for Wireless Ad-Hoc Networks." Paper presented at the Sixth Annual Conference on Privacy, Security and Trust (PST '08), Fredericton, New Brunswick, Canada, 2008.

Shimomura, Tsutomu, and John Markoff. *Takedown*. Hyperion, 1996.

Shneiderman, Ben. *Leonardo's Laptop*. Cambridge, MA: MIT Press, 2002.

"Small Business Size Standards." US Small Business Administration, http://www.sba.gov/content/table-small-business-size-standards.

"Snowball Sampling.". In *The SAGE Encyclopedia of Qualitative Research Methods,* edited by Lisa M. Given Thousand Oaks, CA: Sage Publications, 2008.

Sotirakopoulos, Andreas, Kristie Hawkey, and Konstantin Beznosov. "On the Challenges in Usable Security Lab Studies: Lessons Learned from Replicating a Study on Ssl Warnings." Paper presented at the Symposium On Usable Privacy and Security, July 7 2011.

Spinellis, D. "Reflections on Trusting Trust Revisited." *Communications of the ACM* 46, no. 6 (2003): 112.

Still, Brian. "Hacking for a Cause." *First Monday* 10, no. 9 (2005). http://www.firstmonday.org/issues/issue10_9/still/index.html.

Stryker, Sheldon, and Peter J. Burke. "The Past, Present and Future of an Identity Theory." *Social Psychology Quarterly* 63, no. 4 (2000): 284-97.

Suchman, L.A. *Plans and Situated Actions*. Cambridge University Press Cambridge, 1987.

Sullivan, Larry E. "Grounded Theory." In *The SAGE Glossary of the Social and Behavioral Sciences*, edited Los Angeles: SAGE, 2009.

Teddlie, Charles, and Abbas Tashakkori. *Handbook of Mixed Methods in Social & Behavioral Research*. Sage, 2003.

Thompson, Ken. "Reflections on Trusting Trust.". *Communications of the ACM* 27, no. 8 (1984): 761-63.

Tsai, Janice, Lorie Faith Cranor, Alessandro Acquisti, and Christina M Fong. "What's It to You? A Survey of Online Privacy Concerns and Risks." http://ssrn.com/abstract=941708.

Turgeman-Goldschmidt, Orly. "Hacker's Accounts: Hacking as a Social Entertainment." *Social Science Computer Review* 23, no. 1 (2005): 8-23.

Volken, T. "Elements of Trust: The Cultural Dimension of Internet Diffusion Revisited." *Electronic Journal of Sociology* 6, no. 4 (2002): 1-20.

Vutukuru, M., H. Balakrishnan, and V. Paxson. "Efficient and Robust Tcp Stream Normalization." Paper presented at the IEEE Symposium on Security and Privacy (SP 2008), Oakland, CA USA, 2008.

Wang, Y., S. Komanduri, P. Leon, G. Norcie, A. Acquisti, and L. Cranor. "Ìi Regretted the Minute I Pressed Shareî: A Qualitative Study of Regrets on Facebook." 2011.

Weaver, Nicholas, Vern Paxson, Stuart Staniford, and Robert Cunningham. "A Taxonomy of Computer Worms." Paper presented at the 2003 ACM workshop on rapid malcode (WORM), Washington, DC, 2003.

Werlinger, R., K. Hawkey, D. Botta, and K. Beznosov. "Security Practitioners in Context: Their Activities and Interactions with Other Stakeholders within Organizations." *International Journal of Human-Computer Studies* 67, no. 7 (2009): 584-606.

Whitten, Alma, and J.D. Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of Pgp 5.0." Paper presented at the USENIX 1999, Washington D.C., 1999.

"Windows Local Security Authority Service Remote Buffer Overflow." eEye Digital Security, http://research.eeye.com/html/advisories/published/AD20040413C.html.

Winsor, Dorothy A. "Rhetorical Practices in Technical Work." *Journal of Business and Technical Communication* 12, no. 3 (July 1998 1998): 343-70.

Wu, M., Robert C Miller, and Simson Garfinkle. "Do Security Toolbars Actually Prevent Phishing Attacks?" Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06), Montréal, Québec, Canada, 2006.

Yamagishi, T., M. Kikuchi, and M. Kosugi. "Trust, Gullibility, and Social Intelligence." *Asian Journal of Social Psychology* 2, no. 1 (1999): 145-61.

Yamamoto, T., N. Chiba, F. Magata, K. Takahashi, N. Sekiya, I. Nakamura, M. Ogasahara, and Y. Hashimoto. "Investigation on Anxieties While Using the Internet to Study About “Anshin”." *Journal of Information Processing* 19, no. 0 (2011): 212-20.

Yan, Jeff, and Ahmad Salah El Ahmad. "Usability of Captchas or Usability Issues in Catcha Design." Paper presented at the Proceedings of the 4th symposium on Usable privacy and security (SOUPS '08), Pittsburgh, PA, 2008.

Yee, Ka-Ping. "Guidelines and Strategies for Secure Interaction Design." In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorie Faith Cranor and Simson Garfinkle, 247-74. Sebastopol, CA: O'Reilly, 2005.

Zhang, Y., S. Egelman, L. Cranor, and J. Hong. "Phinding Phish: Evaluating Anti-Phishing Tools." 2006.

Zheng, Saijing, Pan Shi, Heng Xu, and Cheng Zhang. "Launching the New Profile on Facebook: Understanding the Triggers and Outcomes of Users' Privacy Concerns." In *Trust and Trustworthy Computing*, 325-39: Springer, 2012.

Zimmerman, J., J. Forlizzi, and S. Evenson. "Research through Design as a Method for Interaction Design Research in Hci." Paper presented at the Conference on Human Factors in Computing Systems (CHI 2007), San Jose, CA, USA, 2007.

Zurko, M E, and R T Simon. "User-Centered Security." Paper presented at the Proceedings of the 1996 workshop on New security paradigms, 1996.

Appendix A: Survey request

Greetings!

Do you help design user interfaces? My name is Colin Birge, and I'm a doctoral candidate at the University of Washington. I'm running a survey on professional design and development, looking at how design problems are resolved. I would greatly appreciate your feedback.

The survey is open to everyone from UX designers to developers to testers to architects, in any medium: web sites, mobile apps, software, and more. If you have experience with UI design and creation, your input would be most welcome.

You can access the survey at https://catalyst.uw.edu/webq/survey/colinbi/109102 or at http://is.gd/ep1Rn. If you have any questions, please contact me at colinbi@uw.edu.

Thank you for your time, and please pass this along to anyone who might be interested.

Appendix B: Survey protocol

Appendix B: Survey protocol

'Design & Development Survey'

Welcome to our survey on design and development.

This survey is designed to gain insight into problems that are resolved by designers and others involved in the UI design process. This survey will take approximately 5 to 15 minutes of your time.

In general, your name will not be linked to this survey's data in any way. You may be invited to participate in a follow-up interview for this study. If you choose to participate, the study will ask for your e-mail address, in order to contact you to make arrangements for the follow-up interview. Entering your e-mail address is entirely optional. If you choose to enter your e-mail address, that e-mail address will be available only to the primary investigator for this study, will not be used for any other purpose, and will be discarded at the conclusion of this study.

You can withdraw from the study at any time by closing your browser window. Participating in this study should cause no more discomfort than answering a series of questions about your profession.

By clicking on the "Proceed to Study" link, you are agreeing to participate in this study and are affirming that you are at least 18 years of age. Please feel free to print a copy of this consent form for your records.

Thank you in advance for your time! To continue, please click Next.

--

Colin Birge
Ph.D. Student
Department of Human-Centered Design & Engineering

University of Washington

Demographics

For the following questions, please help us to understand your professional experience and the type of organization you work for (if any).

Question 1.

What is your professional title? For example, what title would be listed on your business card?

Question 2.

How long have you been working in your current position?

- ◯ Less than 6 months
- ◯ 6 months - less than 1 year
- ◯ 1 year - less than 5 years
- ◯ 5 years - less than 10 years
- ◯ 10 years or more

Question 3.

How long have you been working in your profession?

- Less than 6 months
- 6 months - less than 1 year
- 1 year - less than 5 years
- 5 years - less than 10 years
- 10 years or more

Question 4.

What are your favorite professional e-mail lists, forums, or other online networking locations? (Optional)

Question 5.

Are you a consultant / self-employed?

- Yes
- No
- No response

Logic destinations

- Yes → Question 7: What is your age? (Optional)
- No → Don't skip (default)
- No response → Question 7: What is your age? (Optional)

Question 6.

What is the approximate size of your current employer?

- Less than 100 employees
- 100 - 500 employees
- 501 - 2000 employees

- ◯ 2001 - 10,000 employees
- ◯ Over 10,000 employees

Question 7.

What is your age? (Optional)

- ◯ 18-24
- ◯ 25-34
- ◯ 35-44
- ◯ 45-54
- ◯ Over 55

Question 8.

What is your gender? (Optional)

- ◯ Male
- ◯ Female

Question 9.

If you were given a code to enter with this survey, please enter it here. If not, please click Next. (Optional)

Design experiences

For the next questions, help us to understand the type of designs you've worked on.

Question 10.

What audience(s) do you typically create designs for? Please select all that apply.

- ☐ Individuals
- ☐ Non-profit organizations
- ☐ Academic institutions
- ☐ Government organizations
- ☐ Small to medium businesses (less than 500 employees)
- ☐ Large and enterprise-level businesses (500 or more employees)
- ☐ Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).

Question 11.

What type of designs do you typically create? Please select all that apply.

- ☐ Web sites
- ☐ Software interfaces
- ☐ Mobile device interfaces
- ☐ Hardware interfaces
- ☐ Games
- ☐ Servers or databases
- ☐ Non-technical interfaces (e.g., maps & signage)
- ☐ Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).

Question 12.

Have you ever worked on a design that gathered or stored personal information (e.g. credit card information, address, financial or health information) from individuals?

	Logic destinations
◯ Yes	Don't skip (default)
◯ No	Survey complete! Thank you...
No response	Survey complete! Thank you...

A complex design example

For the questions that follow, please think of **ONE (1) project** that you have worked on **that required you to gather or store user information**. The more challenging the project, the better.

Question 13.

What type of design project required you to collect this information?

- ◯ Web site
- ◯ Software interface
- ◯ Mobile device interface
- ◯ Hardware interface
- ◯ Game
- ◯ Server or database

- ◯ Non-technical interface (e.g. maps & signage)
- ◯ Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).

Question 14.

What was the intended audience for this design project? Please select all that apply.

- ☐ Individuals
- ☐ Non-profit organizations
- ☐ Academic institutions
- ☐ Small to medium businesses
- ☐ Enterprise-level businesses
- ☐ Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).

Question 15.

What type of user information did the design collect or store? Please select all that apply.

- ☐ Anonymous or pseudonymous information (e.g. user IDs not tied to a real name, aggregated usage data)
- ☐ Real name
- ☐ Phone number, address, or unique government identifier (e.g. social security number)
- ☐ User-created public content (e.g. status updates, public forum posts)
- ☐ User-created private content (e.g. documents not available publicly)
- ☐ User contact list ("buddy list" or address books)
- ☐ Credit card number
- ☐ Other financial information (e.g. bank accounts, financial plans)
- ☐ Medical information
- ☐ Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).

Question 16.

In your professional opinion, how simple was this design problem?

- ◯ Very simple
- ◯ Simple
- ◯ Neither simple nor complex
- ◯ Complex
- ◯ Very complex

Question 17.

Were there specific challenges to this design problem? Please explain. Please do not include any information covered under a non-disclosure agreement (NDA).

Question 18.

What resources did you use to solve this problem? Please select all that apply.

- ☐ Searched the web
- ☐ Asked a mentor or supervisor
- ☐ Asked a co-worker
- ☐ Consulted a reference work
- ☐ Adapted an existing solution
- ☐ Relied on your own design experience
- ☐ Other: Please specify. Please do not include any information covered under a non-disclosure agreement (NDA).

Question 19.

Would you be willing to be interviewed about your experience? The questions will not request restricted information about your design(s) or your employer(s), and your answers will be kept confidential.

	Logic destinations
○ Yes	Don't skip (default)
○ No	Survey complete! Thank you...
No response	Survey complete! Thank you...

Question 20.

Please enter your e-mail address. Your e-mail address will be available only to the primary investigator for this study, will not be used for any other purpose, and will be discarded at the conclusion of the study.

Survey complete!

Thank you very much for filling out this survey. We would be grateful for one more moment of your time. Please pass along this survey link to any professional forums, e-mail lists, or professional colleagues who might be interested.

The survey can be found at *https://catalyst.uw.edu/webq/survey/colinbi/109102*, or at http://j.mp/9RyIOk.

Appendix C: Interview protocol

Notes

These will be semi-structured interviews of varying length. With the exception of the introduction, the protocol(s) described below are deliberately designed to allow for additional questions or for the conversation to be directed by the interview subject.

Introduction

Welcome, and thanks for agreeing to participate in my study on designing user interfaces. I have a few questions about the design process, drawing on your professional experience. The interview should take 30-45 minutes.

As you know, in order to make sure I get an accurate record of the interview, this interview is being recorded. Your name and contact information will not be included with this recording or the resulting transcription, will only be accessible to me, and will be discarded at the end of the study.

At any time, feel free to stop the interview if you are uncomfortable. If you need a personal break, please let me know that too.

While we will be talking about your experiences in the UI design profession, please do not tell me anything that is currently considered confidential or under non-disclosure agreement.

Before we begin and I start the tape recorder, do you have any questions for me?

- When you filled out the online survey in [[month]], I asked you to think about a single, memorable project that required you to gather or store user information. You mentioned, "[Read an excerpt from their answer here.]" Do you remember the project you were thinking of?
- [if no] OK, let's do this then: In the last year, have you worked on any especially difficult projects involving storing user information? Can you think of one in particular?

- What I'd like to do is spend some time talking in detail about the way that you approached the project design. Let's start with some background. It said in your survey that this was a [[type of design]] project for a [[audience type]]. How did the project get started?
- Tell me about the team that helped create this design. Who was involved?
- At what point in the process were you brought in to help?
- How many design iterations did you go through?
- Did the team do any user research? Tell me about it.
- What other resources did you use when you were thinking about the design?
- What did the first iteration look like?
- What changed between that and the final iteration?
- How did you decide on those changes?
- You mentioned in the survey that the project collected [[these kinds]] of user information. Can you say more about the information that was collected?
- Could you tell me about any concerns that you or the team experienced regarding collecting that information? What were they?
- How did you go about resolving those concerns?
- Is there anything else you would like to tell me about your design experiences that we have not touched on?
-

Appendix D: Interview Transcripts

INTERVIEW TRANSCRIPT

2011-0602

Tape No. 110-42602

Interviewer

Colin Birge

Mr. Birge: Thanks very much, first of all, before I get started, I should note, with your permission, I'd like to go ahead and record this phone call so I can get an accurate transcription of it later. Is that okay?

Respondent: Yes.

Mr. Birge: Perfect. So, I have bunch of script that I need to read to start things off, and then we can go from there. Essentially, to give the very brief overview, this is a study on designing user interfaces based on the survey results that you gave me way back, long ago, in November. Thanks for agreeing to participate; that's very helpful. I have a few questions about the design process drawing on your professional experience. The interview is going to take about 30 minutes, or so, 45 max. As you know, in

order to make sure I get an accurate record of the interview, this interview is being recorded. Your name and contact information won't be included with the recording or the resulting transcription. It is only accessible to me and are discarded at the end of this study. At any time, feel free to stop the interview if you're uncomfortable. If you need a personal break, let me know that, too. And most importantly, while we're talking about your experiences in UI design profession, please do not tell me anything that is currently considered confidential or under non-disclosure agreements; I don't want to know. Before we begin, any questions for me?

Respondent: Nope.

Mr. Birge: Okay. Very cool. When you filled out my online survey, way back and long ago in November, I believe it was, what I'd asked you to do was to think about a single memorable project that required to gather some user information and the one that you had picked was one that basically said whether users were going to be okay with providing a full social security number. Let me see if we have additional information about that – and you had said it was from multiple websites and software interface. It looks like that's the most information I have here. Is there – is that a project that you remember; do you remember the project you were thinking of?

Respondent: Okay, I worked for a bank, so that could be any number of things.

Mr. Birge: A lot of things. Okay, then let's do this: In the last year, have you worked on any especially complex or difficult projects involving storing user information; can you think of one in particular?

Respondent: I work on a online account opening; I work on banking. I work on mobile banking. I work on 401(k) applications and

Mr. Birge: All kinds of good stuff.

Respondent: Yeah.

Mr. Birge: For this one, what I'd like you to do is pick one. Pick one project that was especially memorable; that was especially challenging for you.

Respondent: Okay.

Mr. Birge: Okay. Well, then what I want to do is spend some time talking in detail about how you approached that project design; how you approached going at it, so starting with some background, you mentioned that you worked for a bank and you're doing projects for all kinds of different audiences. For the particular project that you're thinking of, how did it get started?

Respondent: Well, most of the projects at my company are brainstormed by maybe a committee, or something like that and then they come down to UX to be fleshed out, you know, what centers are offering and, you know, what we're offering right now and anything – there are a lot of industry reports out there like Forrester and Nielsen Norman & Jayne Sciences and suchlike and things like that from which you can get a lot of information on, you know, on the industry in particular to start to understand how, you know, the people I work for stack up against our competitors. So, like, do you want me to tell you what the project is, or do you want me to sort of talk in the abstract about it?

Mr. Birge: It's totally up to you, whatever you feel comfortable with.

Respondent: Okay. Well, like one project I'm working on right now is mobile banking.

Mr. Birge: Okay.

Respondent: And that one's been a real challenge for me because I haven't done anything with mobile banking before, so there's a lot of challenges that go with it, I mean, you're dealing with, you know, the tiny screens of a feature phone, you know, the iPhone and the Android and the Blackberry and all the different – and then there's the iPhone II, and every Android can have the Android operator and then the Blackberry uses the little wheel vs the ones that are touch, so there's just a lot of , it's not like you can design just one kind of wire frame and do it.

Mr. Birge: Got it.

Respondent: We're good.

Mr. Birge: Yeah.

Respondent: Because there's so many different constraints based on, you know, the different companies that are involved, so

Mr. Birge: Sure.

Respondent: Does that sound like a good one that you'd like to talk about?

Mr. Birge: Yeah, that's perfect. That sounds great. So for this mobile banking project, was this one that the strategist came to your team and said, okay figure out what we should do in mobile banking or was it more specific than that?

Respondent: It's been in the works for awhile, so it's hard to remember back to when yeah, I think it was, just basically, something out there – mobile banking originally came into being in our company –

Mr. Birge: Okay.

Respondent: – but, like for the first platform that we did was the iPhone and there was a real push to, I don't know the exact number, 20 or 30 percent of the market now is Android, so there was a real push to get that out. We treated iPhone, I think, probably the Blackberry then iPhone then Android, but there was real push as you're watching the industry develop the Android, nobody's ever heard of that –

Mr. Birge: Sure

Respondent: – but, of course, there's the price point and things like that so we decided to go with that. It's got a more – a younger, more technologically savvy audience, so I think it's interesting to kind of see the different ways that people are using mobile devices. It's like iPhone people are using it more like an aesthetically-pleasing device, but if you look at the Android, a lot of the applications are different than some of the iPhone ones, and so it's just interesting to--there's no set audience. You know,

you've got, I mean iPhones either can be pretty much anybody; Android's probably going to be people 18 to 25, but there are people 35 that use Androids, and 40-year-olds, you know what I mean?

Mr. Birge: Absolutely.

Respondent: Yeah, so there's much – kind of major challenges. I don't know. Am I going the right way with this?

Mr. Birge: You're doing fine, you're doing fine. This is great information. You were mentioning the fact that it's so hard to know your audience when you've got a broad device – broadly – I won't try to say applicable – but broadly-popular device like the iPhone. How do you cope with that; how do you scope about for an audience when you have that kind of situation?

Respondent: Well, I don't really think about it. We hit upon the solution for that – I mean, we do surveys of our users and you know, a lot of our iPhone users would already be using our online banking products, but more and more people don't want to use online banking and they just want to use mobile banking and stuff like in North Carolina, there are a lot of Hispanic users. There's a large Hispanic population here and they're called the under bank, which means they've got money, but they don't trust banks, and so they do a lot of things with their mobile phones –

Mr. Birge: Interesting.

Respondent: – like, you know, a prepaid card and they don't want to get onto the computer and they don't want, you know, there's also a lot of people that will buy a mobile phone but can't afford a computer, so it's interesting the things like a lot of times banks are already – especially the bank I work for is always kind of going for the higher end consumer, but now, of course, with the economy being in the state that it is, they had a lot to do with it, as well, and you've got to broaden your customer base and in order to do that, you have to be able to, you know, provide offerings that are going to entice people, you know, not only from the wealthy, probably upper class type of people, but you want people who are going to be taking – the up-and-coming people, as well.

Mr. Birge: Sure.

Respondent: Let's see –

Mr. Birge: What was the – when you have designs for things like the iPhone, does the same team work on – for example, an iPhone design vs. an Android design, or do two different teams work on that?

Respondent: Yes, the same team works on it. We've got, you know, I work for a smaller bank, the creative and delivery team is a smaller team so we're a dedicated team. We're probably – there's – I'm the only UX person on it and then there's another designer that actually does the HTML coding and there's a couple other developers that are doing the back end coding as well, so it's – and then there's a whole bunch of managers (Laughter)

Mr. Birge: Of course. Of course.

Respondent: (Laughter)

Mr. Birge: So, do you remember roughly at what point in the process your team was brought in to help. Had the product already been conceptualized or was this a set of user requirements at the time? How did that – what stage did that start?

Respondent: I didn't come on when mobile banking first went out to the Blackberry, I didn't come on until the iPhone, so I can't really comment on that, but I don't think that the UX team was very involved with the Blackberry version of it, and as each subsequent version has come out, we've been getting more and more involved in providing, you know, either the wire frames or feedback, but I think that there's such a rush to get things out, we've got a waterfall message –

Mr. Birge: Yes.

Respondent: – it makes it hard.

Mr. Birge: So, if you're using it, if you're using a waterfall message, you said, or you're not using one?

Respondent: Unfortunately, that's what the company I work at uses.

Mr. Birge: Got it. Okay.

Respondent: So –

Mr. Birge: – so how many design iterations – sorry. Go ahead. Go ahead.

Respondent: So, I've worked for other companies before, but that's what we use now, so, rather than say okay this report is done, you have to say this entire huge part is done, so –

Mr. Birge: Ouch.

Respondent: – it's part of a security thing, so things that go in that, and whatever.

Mr. Birge: Sure.

Respondent: You know.

Mr. Birge: How many design iterations – stages through the waterfall – did you end up going through? For the iPhone, let's say.

Respondent: It's like a continually iterative process, so like I meet with the team, say once a week, to show them what I have now, so you know, like this current thing that we're working on is going to allow you to enroll via your mobile device so I basically have to like, keep people or stakeholders involved so that there are no nasty surprises at the end –

Mr. Birge: Got it.

Respondent: And actually, I had a lot of resistance to getting any – bringing up the idea of people being able to do it – to do enrollment in their mobile device, to enroll in mobile banking –

Mr. Birge: Really.

Respondent: So, it's just been kind of a process of, you know, I'll put forth these ideas and God knows they'll become part of the requirements, so –

Mr. Birge: Got it. So, what was the resistance?

Respondent: Um, it was – I'm trying to think back. I think I just didn't see, as someone who's more technologically savvy, I could see I wouldn't want to go at my computer to enroll in mobile

banking. If I'm going to do mobile banking, I want to be able to enroll in mobile banking and start using it, and so as I was working through, like the computer version of it, you know, the one that you would do on a desktop or laptop, or whatever, it was like, okay, well there's really no reason that we can't do, you know, these things, you know, via the mobile device, and they're just like, you know, they're not going to want to do, I mean a real spot, that they wouldn't want to deal or do that. I think it kind of stems from, you know, what you touched on earlier, which is that each person has this idea of who the audience is and although we started developing incentives for our entire user base, we don't have particular systems yet for, you know, iPhone and our Android and our Blackberry users, or Windows Mobile 7 or Palm 3 –

Mr. Birge: Sure.

Respondent: – so, that's a lot of – that's one of my goals is to try to get that information so that we can, you know, get over the expectation of what these kinds of people are looking for and the surveys are helping me to do that, but obviously, being able to talk to clients is more helpful if you can find them, but it's sometimes difficult in a banking setting to be able to get access to your clients.

Mr. Birge: That makes sense. How do you work around that? Or work with that, perhaps?

Respondent: Yeah, I guess you just kind of do your best guess of how things should work. Do your survey, provide the best customer experience-- .

(Personal aside to someone in the room.) Sorry about that.

Mr. Birge: No problem. What – how you deal with – problems getting access to your clients in some cases.

Respondent: Yeah, in some cases you don't have access to them, so you just provide the best experience that you can, given what you know about the medium that you're providing the experience in, you know –

Mr. Birge: Sure. Okay. And then when you say, given what you know, so, you're thinking there of prior experience of design or, what are you thinking of?

Respondent: No, that's another challenge. well you can be an expert in any – something, like the web–

Mr. Birge: Sure.

Respondent: You can go out on the web and look and go, oh, I understand that and now I know what to make, but because it's harder to get to the things on the phone and you're only going to have, like, even if you have an iPhone contract, you're only going to have an iPhone contract. You're not going to have an Android contract or a Blackberry contract or Palm III-- so it's also hard to get the device expertise. Do you know what I mean? There's tools out there like Device Anywhere, but one of the main limitations of that is that you're looking at just gesture-based interfaces and a device anywhere is you take a mouse and you try to figure out what a mouse click or drag corresponds to, you know, in tapping the screen – see what I mean?

Mr. Birge: Sure.

Respondent: And it also, you know, touch base interfaces, you can't test for, you know, the sensitivity of the screen. You know, our click-based interface is different, so it's hard. We have to go, like if I don't have access to two of the devices and I can't borrow one, I have to go to the store to look at them.

Mr. Birge: Understood.

Respondent: So –

Mr. Birge: So, that's actually kind of an interesting question, right? You have – we were talking about the resources that you need to work on your design, essentially, so you have access to the clients to the extent that you can and the survey data to the extent that you have it – either physical access to the device or access like something like a device anywhere that at least lets you do some level of development. What other kinds of resources do you use?

Respondent: I think that's about – I mean, there's a lot of books out there that you can read, and I have a friend who likes the iOS Guidelines and the Blackberry guidelines, and Android, and they've got some out there that are helpful, especially the Apple one – there's a lot of books on mobile devices and just how in general, people, you know, psychologically – the psychological issues that come from trying to get all the information in the small screen, and then there's a lot – I think just reading about that, so I don't think I can count on that. There's just a lot of information out there so that's truly what my main source is, so you know, if I can't find it on the web and I can't get it through the devices, I'll just read books on it.

Mr. Birge: Sure. Now, is there a particular book or books that's your go-to books – that are a reference?

Respondent: I wouldn't say one that is always a reference. There's a couple of good books – I don't know the name of one of them off-hand. I'm reading it, actually, right now, but I like *Tapworthy*, that's about iPhones, for some stuff. It's more general, but, I mean I don't think there's a lot of definitive stuff out there that's easy to find. You have to wade through to find stuff that, it's really, you know, beneficial to use and worth the money. [*Tapworthy: Designing Great iPhone Apps* by Josh Clark (Jun 25, 2010)]

Mr. Birge: What's – when you're working through your design process, obviously, you're making changes as you go, what's the process for deciding on what those changes are?

Respondent: Well, normally, I would run like the screen splits that I was thinking of. I would have already worked out, a high level of diagramming, flow charting some of the process with the stakeholders, especially the designer, and the developer, and then I would bring, you know, screen by screen, you know, wire frames or simulations, to the stakeholders because, honestly, these are the products that they work with every day and they've got a lot more interaction with the clients and then with mobile banking, you need to deal with the online banking people and you need to deal with the

online accounting people, I mean there's a lot of different systems that are involved. And so, then I basically go through the simulations, make notes and explain everything and make sure – I go, is anything wrong and do they have any new things and haven't changed their mind on anything and if they have, I, you know, iterate until everybody's like, okay! (Laughter) It's a long process!

Mr. Birge: It sounds like it. You mentioned the stakeholders. Who all are they? What are their roles, I should say?

Respondent: There are many stakeholders; there's the online banking people, there's a whole team with that. There's the people like the manager from mobile banking, there's the manager for alerts, there's the manager on top of them and the managers on top of them. There's marketing. Let's see, I mean, the indirect stakeholders would obviously be the managers that are, you know, over our team, over the entire thing, you know, and are affected by the revenue that mobile brings in. Who else is in there? It seems like there's just about everybody.

Mr. Birge: Fair enough.

Respondent: And the, the copy writers need to be in there – and I'm trying to kind of work my way through a meeting room and figure out who all from that is there – there's likely to be the testers, the QA team in there, so I think that's pretty much everybody.

Mr. Birge: Fair enough. Changing the subject a little bit, what kinds of user information would your mobile program collect, so if it's starting – if you're starting a bank account, what kinds of things do you need to collect for that?

Respondent: We don't currently have them for starting bank accounts, but if you wanted to sign up for online banking, we would need to collect information about how, like if you're a client already, and if you are a client already then we need the account information to identify you.

Mr. Birge: Got it.

Respondent: And if you're not, then we would have to direct you right now to the computer, basically, because the online account, at least, isn't on the mobile device.

Mr. Birge: Fair enough. When you say "account information" is that a log-in and password or something more complex?

Respondent: It depends on what kind of client you are. I mean, it could be your account number. It could be a debit card number, it could be a PIN number. It's not your Social Security Number – well, for certain types you might have to have a Social Security Number, and, like your ZIP code and then you create your user ID and password. For – if you're like a client who we can't ascertain your identity because we don't have – you don't have an account number and a PIN number, because you don't have those, then we just send you to Lexus Nexus, so there's a lot of information that needs to be collected to make sure that you are who we think you are.

Mr. Birge: Got it. So what concerns did you or the team have while you were collecting that information, if any?

Respondent: I don't think we had any concerns as far as that because we actually were collecting – it was something that online banking was already doing, so we were just piggy-backing on that process, but I do remember back when I was doing online account opening, that there was a real concern that, at the time, you know we were making up numbers like a Social Security Number and a PIN, or something like that and there was a real push to get people to, you know, to move people away from having to find their whole Social Security Number.

Mr. Birge: Sure.

Respondent: Or even the last five of the social – you can find other identifiers besides that. And the same thing with a 401(k) application, you know, we moved everything away from the use of the Social Security Number and a PIN to you know, creating a user ID and password as your log-in credentials. Some of the older systems, you know, were looking for different types of credentials to work

with, that were too sensitive to be asked for on a regular basis or transmitted on a regular basis, you know, just for the logon.

Mr. Birge: Sure.

Respondent: Does that make sense?

Mr. Birge: It does. So, in terms of – it sounds like the issue was in terms of finding a log-on that would uniquely identify them without actually invoking something like a government identifier, or something that could be used or misused more broadly.

Respondent: Right. Right. And I think for this particular project, like we've already addressed that for other projects and so the question of, you know, what information we should be getting is not a problem.

Mr. Birge: Got it. Fair enough. Is there anything else you would like to tell me about your design experience that we haven't touched on?

Respondent: I don't think so.

Mr. Birge: Okay. Fair enough. I like to ask. Thank you so very much for taking the time tonight. I really do appreciate this. It will be a great help for my study.

Respondent: Oh, good! Are we going to get to see your study? Eventually?

Mr. Birge: Eventually. Yes. I am in dissertation-writing mode, so it's going to be later rather than sooner, but it's coming.

Respondent: It's going to be years?

Mr. Birge: Oh, gawd, please don't say that! It's going to be months rather than years, but it's going to be months, but it's coming.

Respondent: Well, good. And good luck with it.

Mr. Birge: Thank you. Thank you very much, and have a wonderful evening.

Transcriber Certification

I, Lee Baxter, hereby certify that the enclosed transcript prepared by me is a full, true and correct transcription of the Recording 110-42602 provided by Colin Birge. I further certify that I have no interest in the outcome of the project.

Entered this _____ day of _____, 2013.

Lee Baxter

15832 NE Leary Way

Redmond, Washington 98052-4329

206-650-7640

INTERVIEW TRANSCRIPT

2011-00602

Tape No. 110-40603

Interviewer

Colin Birge

Mr. Birge: . . . very good. Can you hear me okay?

Respondent: Yeah.

Mr. Birge: Perfect. So, what I wanted to do was to follow up on the study that you took, unfortunately several months ago now, on designing user interfaces and basically I had a brief set of questions that we're going to go into in a little more depth about the design that you had told me about in the survey, if that's okay. It'll take about a half an hour, or so, of time. Is that fair?

Respondent: That is fine.

Mr. Birge: Perfect. So, first off, I have a brief script I have to read. I apologize for the formality of it. Welcome. Thanks for agreeing to participate in my study on designing user interfaces. I have a few questions about the design process drawing on your professional experience. The interview should take about 30 to 45 minutes. As you know, in order to make sure I get an accurate record of the interview, this

interview is being recorded. Your name and contact information won't be included with the recording or the resulting transcription. It will only be accessible to me and will be discarded at the end of the study. At any time, feel free to stop the interview. If you need a personal break, please let me know that, too, and most importantly, while we will be talking about your experiences in the UI design profession, please, please, please do not tell me anything that is currently considered confidential or under known disclosure agreements. I don't want to know.

That's the script. Before we begin, do you have any questions for me?

Respondent: No.

Mr. Birge: Okay. Very cool. When you filled out the survey which was embarrassingly long ago at this point, you had been talking at the time about a project that involved credit card security codes. Specifically, you mentioned that there was some complexity around getting the security code giving differing location on different types of credit card, right?

Respondent: Right.

Mr. Birge: Do you remember the project you were thinking about?

Respondent: Yeah. Sure.

Mr. Birge: Okay. Very cool. What I'd like to do is spend some time talking in some detail about the way that you approached that project design, so to start with some background, it was not immediately clear from the survey data what this was – it looked like a voice speak user interface of some kind meant for individuals. Is that correct?

Respondent: That's right.

Mr. Birge: Okay. Can you tell me a little bit more about it?

Respondent: Yeah, sure. This was for – you know, there's a type of module called pay-by-phone?

Mr. Birge: Okay.

Respondent: Okay. I don't know if you ever, you know, conduct transactions using automated systems over the phone.

Mr. Birge: Absolutely.

Respondent: But, you know, you probably have paid by phone once or twice –

Mr. Birge: Sure

Respondent: – so there's a standard of bits of information that you need to collect and in this particular case, this was – let me think – probably around 2000 – 2001, something like that. So, those hadn't been – they weren't as ubiquitous as they are now.

Mr. Birge: Got it.

Respondent: And then, you know, of course trying to design this for use with a speech system rather than a touch-tone system, it was already running as a touch-tone application, so the goal here was to change to speech and try to smooth things out.

Mr. Birge: Interesting. Very cool. How did the project get started?

Respondent: Well, you know here, projects in the department I work in – I'm one of two speech-user space designers. We've got programmers and a couple of project managers and the project managers are out there, you know, checking around trying to find work and when they snag a project and pull it in, they go through all the paperwork and then once we got the authorization to start work, then you know, they pull the team together.

Mr. Birge: Got it. So it was launched by the project manager based on some external feedback.

Respondent: Right. We're pretty much a consulting group.

Mr. Birge: Got it.

Respondent: So, this was not something that was being developed for our company, but something we were developing for someone else.

Mr. Birge: Got it. Okay.

Okay. Very good. What's – tell me about the team. You mentioned that there were project managers involved and that you, yourself, are a speech UI designer. Who else was involved in thinking through this design?

Respondent: Well, in this case, as I mentioned, there was an existing design touch-tone –

Mr. Birge: Sure.

Respondent: So, a lot of the elements – a lot of the task analysis had already been carried out, and so this was a working touchtone module. So, given that, I would say that, you know, probably, one of the first steps is for one of the designers to analyze it and, you know, given our background in speech and communication theory and things like that, to take a look and, you know, re-script the interface.

Mr. Birge: Can you say more about what you mean when you say "re-script"?

Respondent: Well, yeah. You know with touchtone, you going to have choices where, you know, you'll have, you know, for A, press 1, for B, press 2 –

Mr. Birge: Okay.

Respondent: – that type of thing. Now, how can I put this – you know, in a lot of ways, there's nothing – I've got to think about the right way to put it. A lot of times, touchtone interfaces are just not carefully done. They're scripted by people who don't have a deep understanding of the people who are going to be using it.

Mr. Birge: Okay.

Respondent: And the language tends to be clumsy –

Mr. Birge: Okay.

Respondent: – clumsier than it has to be. And, consequently, the interactions going to be less efficient than they can be. For example, a common mistake is, you know, writing full sentences for everything. You know, it seems right on paper, but it's not conversational and not efficient.

Mr. Birge: Sure.

Respondent: So, one of the first things to do is to go through and, you know, take a look at how things are being expressed, currently in touchtone, and then when you're doing a conversion to speech, you need to figure out how to re-express those so a bad speech system would be one where you simply change to a, you know, a press or say type thing for A, press or say "one", for B, press or say "two". While that's, you know, the most direct translation from touchtone to speech, but it's far from conversational and far from efficient.

Mr. Birge: Sure.

Respondent: So, you know, without going into lots of detail of design, you take a look and link the menu so you might express those as a single sentence. You might need to express them as a, you know, a longer set of choices. There are ways to do that, and then this particular design problem, you know, you're collecting, you know, strings of information and amounts and things like that. When it comes to the security, the CCD code, well, you know, it's in different places on different cards. AmEx is on the front, VISA is on the back. Three digits on VISA, four digits on an AmEx, and at the time that we were developing this, on the back of a VISA it might not even be there at all. There might not even be a CCD code.

Mr. Birge: Oh, I see.

Respondent: They're ubiquitous, now, but at the time we were building this, you couldn't count on it being there.

Mr. Birge: Interesting.

Respondent: So, anyway – so when I talk about re-scripting, that's, you know, first off, taking a look at what's currently being done and, you know, figuring out how to do that without actually requiring people to press buttons, and to, you know, make it the best, most engaging conversational scripting that you can do. So, as far as development tasks would go, that's one of the things that the

speech interface designer would do was to go through and do that. Once you got an idea about how you wanted this to go – have you ever heard of voice XML?

Mr. Birge: Tell me more about it.

Respondent: Well, it's like HTML, but the tag – the tags are different.

Mr. Birge: Okay.

Respondent: But the thing about it is that if you have a voice XML compliance speech browser which would you have, you know, a speech recognizer in it, the ability for producing speech with text-to-speech?

Mr. Birge: Sure.

Respondent: Then you can – what voice XML does is make it easy for someone who's not a programmer, like me, to create prototype things –

Mr. Birge: Oh, okay.

Respondent: – so, I'm able to – so one of the other things I would do is take the proposed scripting and then substantiate it as a voice XML code type. You know, it wouldn't actually make contact with any real data bases just because that takes a real programmer, but you can certainly fake the interaction in such a way that you can get your prototype running and then, you know, bring other folks in and go through utility testing with the prototype.

Mr. Birge: Okay.

Respondent: So, anyway, those are all the kinds of steps that I was going through with this particular thing and that's how, you know, one of the things we now – you know, basically, that was how – you know, trying to figure out how to express this – I think those are pretty much the steps that I went through to try to get to a point in what we felt we had a nice solid design, and then that would be handed over to the programmers in the group who would, you know, use more sophisticated and, you know, hard development techniques to get to the actual code that was employed.

Mr. Birge: Did you have anyone else working with you directly when you were in the process of the re-scripting or development of the prototypes?

Respondent: Working directly with me – no, that was pretty much of a solo activity.

Mr. Birge: So, essentially, you took the earlier design – the touchtone design, went through the re-scripting exercise, developed the prototype, ran some use-ability tests to verify the prototype, and then handed it off, in turn, to the programmers.

Respondent: Right.

Mr. Birge Fair enough. Did you have any input once the design had been handed off to the programmers, or was it essentially off your plate at that point?

Respondent: Well, in this particular case, I don't remember a lot of back and forth on that specific one. But in general, when we do something like that, then it will eventually go through acceptance testing with the client, and then, you know, once it's gone through acceptance testing, after deployment, issues may arise also.

Mr. Birge: Sure.

Respondent: And on some projects, you know, things will come up where, you know, I get pulled back in. We have to figure out what to do to solve a particular issue that's come up that, you know, the other things that we went through didn't catch.

Mr. Birge: How many design iterations did you end up going through as you were doing your re-scripting?

Respondent: On that one – well, you know, I had one, two, I'd say about three.

Mr. Birge: Okay.

Respondent: And that includes, you know, taking into account the usability testing.

Mr. Birge: What is – how would you characterize the iterations; were they more formal? Were they more informal part of the process?

Respondent: I'd say more towards the informal.

Mr. Birge: Okay.

Respondent: And the usability testing itself, was more formative than summative.

Mr. Birge: Got it.

Respondent: You know, not large sample sizes, but you know, getting a few people through and just, you know, getting a sense of whether or not, you know, whether or not there was anything that was tripping people up.

Mr. Birge: Um-hmm. What resources did you use when you were thinking about the design, if any. You mentioned usability data.

Respondent: I'm sorry. Say that one more time?

Mr. Birge: So, you mentioned that ran some usability testing and got some formative information that way. What else informs, if anything, what other resources did you use. What else informed your thinking about the design that you were creating?

Respondent: Okay. Well, for these types of designs, you know, the – almost the fundamental activity is the scripting. And that involves scripting code in the sense of what you might think of the primary path through the interface, you know, what you really expect people to hear and if they respond successfully to it they move to the next step and, you know, try to get them through the automated process. You also need to have your fall-back scripting in place in case somebody gets tangled up somewhere along the line.

Mr. Birge: Sure.

Respondent: So, the resources there are basically literature – research literature that's available, I'd say from a couple of different areas to think about. One is understanding how the technologies work; what you can and can't do with the current speech-writing mission. The other is from psycholinguistics and pragmatics in communication theory which, you know, you've got these huge

bodies of research that provide guidance on how to – how the system should, you know, should talk to the user. And, then, there's this whole area out of market research that's called service science, where these are things that – these are all kinds of entangled a little bit, too. A lot of the stuff in Service Science comes to what are the appropriate ways to speak to someone when you're talking about the social roles, such as provider and client, so you know, at any point you make in your scripting decision, given the way human language is, they're probably infinite. You know, a set of choices you can make –

Mr. Birge: Sure.

Respondent: – are guided by, in this particular kind of case, you know where you are providing a service to a person who pays money to you, then you need to pay attention to the kind of wording that is socially appropriate, but you also don't want to get so tangled up in editing that you forget that it is part of the service provider relationship or what makes someone an excellent service provider is efficiency; you value the other person's time. There's room for variation. There's certainly, you know, I wouldn't call it totally guesswork, but there's more than one way to do it. But, at some point you have to make a decision because there will be only one product.

Mr. Birge: Right.

Respondent: But then, of course, that's where, you know, some usually testing – some sort of feedback, will play that role.

Mr. Birge: Going back to your discussion of the three iterations, as best you remember, what the changes that took place – say, between the first and the third? What ended up differently

Respondent: Well, certainly, one of the things that ended up differently was, you know, I clearly remember as coming up in usability studies were the difficulty of trying to figure out the most efficient way to get the security codes – CCD – from the caller, particularly given the possibility that it might not be there, so one of the first questions that we originally asked was, you know, something like

AmEx is a lot easier because it's very consistent but if they selected VISA as their payment type, then we had a question of, you know, is there a three-digit code on the back of the card?

Mr. Birge: Right.

Respondent: And at the time, we had the grammar written just basically a yes/no grammar, you know, a yes and no and a number of variances on that, but again, you know, as soon as people started doing this, you know, it was like, you know, slapping myself on the forehead. I would say, look at that. Instead of saying yes or no, there would just be numbers. Well, that's because if they just said three numbers, that was as good as a "yes" and it saved a step.

Mr. Birge: Sure.

Respondent: But the system would just say please say yes or no, so that was something that we had to fix across the iterations, so that the grammar instead of just being yes or no was also aware of the possibilities that somebody might simply speak three digits.

Mr. Birge: Interesting. Interesting. Any other kinds of changes that were made between the first and the last?

Respondent: You know, I doubt it. I don't really remember having to make lots of changes, but that's one that really stands out, because that's the kind of thing where you're kind of saying, no, I really should have anticipated that happening.

Mr. Birge: Absolutely. In terms of collecting credit card security codes, I mean obviously, this was considered to be – it might be considered to be private, were there any special concerns or special considerations given in terms of the design for that?

Respondent: Well, that certainly is a place where you would not require someone to speak the digits. So, as far as, you know, and actually, now, you know, ten years later, it's very common in speech interfaces to, you know, recognize first off, you normally might be saying long strings of digits, you know, one misrecognition and, you know, blows the whole thing. For a lot of the types of things you ask

somebody to enter, there are some privacy issues, so you usually allow that entry to be touchtone as well as speech.

Mr. Birge: Got it. Was that the norm at the time, ten years ago?

Respondent: At the time, I don't think we really thought about it as much. I'm pretty sure that the initial scripting – I'd have to go back and look at the scripting. I can't remember. Doing it now, there would be no question you would set it up in such a way that you made it clear you could speak or enter the digits, but I don't recall.

Mr. Birge: Fair enough; interesting. You mentioned how you would do it now; do you see any potential improvements in the future?

Respondent: Well, yeah, it was – it did what it was supposed to do. I guess the kind of improvements to look at currently would be that, you know, once you captured information and permission to store it, so on subsequent calls you wouldn't need to go through that, you'd ask, you know, something like do you want to use the same card you used last time –

Mr. Birge: Sure.

Respondent: – you know, possibly mentioning, you know, the last four digits of the counter, or something like that. You wouldn't want to lock somebody into a particular credit card, but you would also want to try to take the steps for payment as painless as you can.

Mr. Birge: Absolutely! Interesting. Okay. Is there anything else? This has been enormously helpful. Is there anything else that really comes to mind when you're thinking about this particular design that represented kind of a unique challenge or something uniquely peculiar about this particular one?

Respondent: No, other than – nothing else really comes to mind. I mean, no – just as, you know, I don't know if it's helpful, but you know kind of another surprise that happened on a different project – this was a reservation – this was for doing reservations, and it turns out that for reservation systems, well, you know, there are some complexities associated with deadlines –

Mr. Birge: I'm sorry. I missed the last term.

Respondent: There are some complexities associated with midnight.

Mr. Birge: Oh. Okay.

Respondent: That's the zero. So, what do you say, if someone says they're going to pick something up at midnight, then you know, that makes the date ambiguous in some ways. I mean, they'll tell you the date, at midnight, and you're still not sure, but – so – but another thing that happened was, you know, you can't have a reservation system the first time through, we built the time grammar, so that, you know, you'd ask the person, you know, where are you going to pick up the car? And you know, somebody will say 11:30 a.m. and that works fine; or say, 12:30 or 2:30 p.m., that works fine, too. But it actually turns out that people get a little uncomfortable with Twelve, so rather than say "12" if they're going to pick up at noon, you know, quick, they say is that 12:a.m. or 12:p.m. You've got to think about it a little bit, so they just say "Noon" and I didn't have that in the grammar, so easy to fix.

Mr. Birge: Interesting.

Respondent: So, just the kind of thing that, you know, another one of those little peculiarities that, you know, you just need to take into account.

Mr. Birge: Interesting. Dr. _____, thank you so much for taking so much time for me this afternoon. I really do appreciate it.

Respondent: Yeah, Yeah, that's fine. Good luck with everything.

Mr. Birge: I appreciate it. If you have any other thoughts of stories you'd like to add, or things you'd like me to know about this project, you have my email address, so by all means, send them along. I'd be very interested in hearing them.

Respondent: You bet.

Mr. Birge: Thanks again. Take care.

Respondent: Okay.

Mr. Birge: Bye-bye.

Transcriber Certification

I, Lee Baxter, hereby certify that the enclosed transcript prepared by me is a full, true and correct transcription of the Recording 110-40603 provided by Colin Birge. I further certify that I have no interest in the outcome of the project.

Entered this _____ day of _____, 2013.

Lee Baxter

15832 NE Leary Way

Redmond, Washington 98052-4329

206-650-7640

INTERVIEW TRANSCRIPT

2011-0602

Tape No. 110-40801

Interviewer

Colin Birge

Mr. Birge: . . . Okay, then, can you hear me?

Respondent: I can, yes.

Mr. Birge: Okay, so a moment here for modern technology, so what I wanted to talk with you a little bit was the experience you've had and the survey you did a few months ago – an embarrassingly long time ago – but before we do that, in order to keep human subjects happy, I do have a short little introduction that I need to read off to you, so bear with me. Welcome. Thanks again for agreeing to participate in my study on designing user interfaces. I have a few questions about the design process, drawing upon your professional experience. The interview should take about a half an hour or so, possibly shorter or longer, and in order to make sure I get an accurate record of the interview, this interview is being recorded. Your name and contact information are not included with the recording or the resulting transcription and are only accessible to me and will be discarded at the end of the study. At

any time, feel free to stop the interview. If you need a personal break let me know that, too. And most importantly, from my point of view, while we're talking about experiences you have in the design profession, please do not tell me anything that is currently considered confidential or under non-disclosure agreements; I don't want to know. Before we begin, do you have any questions for me?

Respondent: No, it sounds pretty straightforward.

Mr. Birge: Okay. So, when you filled out the online survey way back and long ago, I asked you to think about a single memorable project to gather or store user information. One you had talked about – you said that there was a site that was taking donations from people for an operatic society.

Respondent: Ah, yes.

Mr. Birge: That users could opt to donate for certain types of funding and that there was some challenges in matching donations with intended usage. Do you remember the project you were thinking of?

Respondent: Yes, Seattle – the Seattle Opera.

Mr. Birge: Very cool. So, what I'd like to do is spend some time talking in detail about the way that you approached the project design, so to start with a little background, it said in your survey that this was a website project that was targeted at and essentially individuals as opposed to academia. How did this get started; how did the project get started?

Respondent: Well, at the time, I was working at an agency and basically, the opera needed some system by which patrons of the opera could donate online and become a funder in that they wanted it to, you know, not just say thanks very much, but kind of tier the funding and give feedback as in they could sponsor specific things for example, so basically, they could see what they were funding rather than just anonymously handing over a check and saying thanks for the money.

Mr. Birge: Sure.

Respondent: So, that's how that came about. And the way we tried to approach this problem was for one establishing with the client Seattle Opera Company in this example, establishing what kind of information they wanted do they want to give, what kind of donation levels they wanted to establish, and how can we create an interface that would give people the options to choose what they would like to fund and basically give that feedback going through the process of going through an online form to set up this funding cycles, so we approached it in – a couple of problems – how was the Seattle Opera Company, who don't really have technical teams to update this information – how would we have them update this information, create tiered funding, funding options without, you know, having to call up the interactive agency just to make simple text updates.

Mr. Birge: Sure.

Respondent: Kind of non-technical information for the user to look at, so we came up with an XML based solution with… – I don't know know if you need the more technical aspects or the more UI aspects.

Mr. Birge: Whatever you'd like to tell me. You came up with an XML-based solution.

Respondent: Yes, so we came up with an XML-based solution, well, and we would update a sheet, like an XML file, which is basically just a text file with whatever they want to put in there and we had to design a UI back-end solution depending on what was in there. Those were the options, Say there were options A, B, or C. If they wanted to, they could add a D and that would be displayed on the front-facing web site. He could choose D if they wanted to fund costuming or something like that. They would have that option up there and wouldn't have to contact us to make that happen, so we had to sort of create a scalable solution in that sense so that we could offer as few or as many things as the client wanted.

Mr. Birge: Yup.

Respondent: And the next thing we had to do was create a form that they could—that it was kind of very manipulatable, I don't know if that's a word, but depending on what they chose, different information would be displayed. They could choose D and it would give information about what kind of costuming, you know, an overview of what that costuming would actually do, and then if they chose C instead, they would get more information about that. We could remove that information and display the correct information depending on what the user wanted. And then basically take them through the steps to making sure the process was linear so that he would understand that we started off with making the choice of – excuse me – the direction – the next step would be how much would they want to fund the donation and the third step was the actual financial information, so we had to create a linear kind of process so it was very simple for the user to go from step one, step two, step three without it being a confusing experience, especially because the demographics were some people who might be funding this kind of a cause or organization are likely to be in an older demographic it was opera-related – it tends to be an older demographic –

Mr. Birge: Yup.

Respondent: – so we had to kind of make it as simple as possible and not too many bells and whistles but at the same time sophisticated enough so that we could get information processed and user identified.

Mr. Birge: Right. Very cool. Tell me about the team that helped create this design; who was involved?

Respondent: Okay, something like – we tend to have – you've got to have many aspects to the team. To start with, you have a kind of a client manager or account manager, who initially speaks with the client and establishes what their need is. They normally come back to the technical editor or the UX architect, the users' experience architect who works out how we can actually break this down and make it happen. They would normally create some wire frames so that we could see that we need three pages to

be built and on each page this is going to happen, so basically just the actual user experience and the interaction that will take place. Once that has been established, normally we get approval from the client at each step of this. Once the wireframes have been established it will be turned over to the graphic artists, they will create a composition of what the page will look like. The next step after that is generally, when my kind of role came in for this particular one, in that I would be developing at the front end, the actual interface into code kind of thing –

Mr. Birge: Sure.

Respondent: Normally, when I should probably back up a bit – so from to the UX architect, we are actually involved in that aspect to a degree, they'll say to do this and we will say, well that can happen, but we need – we kind of have a consensus on what the various technical elements will do inside of that wire frame and is it feasible. Some people may want things that wouldn't exactly be – the technology wouldn't work with the intention. I think that might be the way of putting it, so we kind of all had to agree upon that before it gets to the graphic artists and then I worked with the graphic artists again, graphic artists are UI designers making a project background. We'd work with them to say this will be able to work, actually becomes that interaction, and then in that situation I would be at the front end of everything and then normally some software development questions to capture the information that would be put into the application by the user such as the credit card details, all of that stuff, so all of that would be at the back end.

Mr. Birge: Got it.

Respondent: So, the account manager, UX architect, graphics designer, front-end development, software developer four or five roles split up among different people.

Mr. Birge: Makes sense. Very good. At what point did you get brought in? You mentioned that you came after the project had been established, the wire frames had been sorted out. Did you have any influence earlier on in the project?

Respondent: I came in pretty much as the UX architect started the wire frames. There were initial discussions about what was needed and basically that three pages was a multi-faceted discussion between the graphic artist, the _____ developer and myself, so that was kind of my first point of entry.

Mr. Birge: Sure.

Respondent: I was coming in then so before the wireframes was created there was discussion get input from all aspects about how this would be built out.

Mr. Birge: Got it. How many iterations do you think you went through in that process?

Respondent: (Laughter) I can't remember. Definitely more than five.

Mr. Birge: Got it.

Respondent: I would say more than five just because a lot of these iterations, before it gets to the graphics designer, there were a couple iterations after, they'd be reworking on it and we'd receive feedback from the client to change a couple of things, but the main amount was at the very start of it, otherwise you know, it doesn't come out of the UX architect shop until we had a 90% solidified design –

Mr. Birge: Sure.

Respondent: Otherwise, you know, back to the drawing board and a huge waste of resources –

Mr. Birge: Yup. That makes sense.

Respondent: I would say certainly more than five from that end of it and there were probably edits from the graphics designer and myself, so probably when we were through, about ten.

Mr. Birge: Okay. Fair enough. Did – in the course of going through these design iterations, you mentioned a couple of essentially client reviews. Did you do any other kinds of user research or talk to anybody who would be using the system?

Respondent: In this situation, we didn't, but I have done those before when we did some testing but in this particular one, there wasn't any of that in it. Kind of a – it wasn't the first time the

agency had created something like this for a nonprofit, so they kind of had a pretty good model to start with, so that was – I mean, they had the kind of a basic model of how people respond to this stuff. So basically, it was drawing upon earlier experience of how people like a more linear process in you know, donating money or any kind of e-commerce model, and just using those practices within the design.

Mr. Birge: Got it. Makes sense. So you mentioned that you had this existing model that the agency was using for pushing this through. Were there other resources that you called on as you were building out this design?

Respondent: I think that in general, there were a few best practices used – or should be used, I should say – kind of industry-wide, especially where it comes to people say, either donating money or buying something online. You know, creating a really less-confusing process, making it straightforward and a clearly marked process so that the user knows what they're doing and when. Those iterations being drawn are probably more general industry stuff so other than the agency's particular experience or something like that, we were just drawing on general industry practices and guidelines and our own experience.

Mr. Birge: Got it. What changed between the first iteration and the final iteration insofar as you remember?

Respondent: I recall there were initially more pages – I remember initially what they wanted to do was to create on the landing page, they wanted to create a different page for each type of thing that they wanted to sponsor –

Mr. Birge: Sure.

Respondent: – so that they would sponsor different touring groups and if you click on that you would get a whole different page. This proved to be a bit impractical, one because people would be clicking backwards and forwards constantly just to see what options there were, the final ended up having that appear on the actual page via Ajax. So that was the initial idea of having several pages but

because of what we mentioned before about finding sponsorship pages. It was a bit of a cumbersome idea, so we managed to get it down to just one page with the content being refreshed on that same page.

Mr. Birge: Got it.

Respondent: That was one of the big ones. A couple of other ones were just _____ very tech savvy, so with the text when they're explaining the different kinds of donation types – so some kind of practical experience-based changes. There were quite a few little look and feel changes that were made along the way things being aligned in different areas.

Mr. Birge: Makes sense. Very cool. How did you decide on – sorry, go ahead.

Respondent: Most of the changes were actually feedback from the client, I should add, and that happens more often than not. You know, they're fine with the function, but just a little bit more or a little bit less. That's probably a large part of our changes, normally client requests.

Mr. Birge: Yes. So in the you mentioned client requests that drove some of the look and feel changes. The other changes were driven by what, by the flow? Or what caused you to make those changes?

Respondent: Well, it just, as we mentioned before, we tried to make it as linear straightforward a process as possible, so looking at it initially, basically we kind of like, more of a brainstorm session where we thought, we could create different pages for different things, but you know, we went backwards and forwards with the landing page. It would not be the greatest user experience. I guess what drove that was just was our own experiences online and so forth, what are the different technological solutions that will create the smoothest experience. And as we brainstormed, we got to things like using Ajax to refresh the page with relevant content.

Mr. Birge: Makes sense.

Respondent: Yes, and you know, and we just looked at what technology do we have, what can we do to make it a good experience.

Mr. Birge: Perfect: You mentioned in the survey that that was collecting essentially financial information so phone number, address, government ID, credit card, that type of information, and this – just to be clear so that I understand – this was primarily information you were collecting – just to process the actual donation itself.

Respondent: Yes. There wasn't really data mining going on, we weren't being Facebook about this. It was purely just so they could process the financial transactions. There wasn't anything other than that. Also so they could send out marketing, which we had opt-in options for, receiving e-mail newsletters and so on. They also, the opera company would be giving updates, as they were becoming a donor, there would be some marketing involved, there were options based around whether or not they would become a donor.

Mr. Birge: Got it. Understood. Were there any concerns that you or the team had about the design of the UX that collected that information?

Respondent: No, we were pretty happy with the whole thing. We were very well-versed in the using the secure systems for collecting that information and making sure it wasn't anything that was prone to identity theft or anything like that. That was more the software developer's world. If there was a concern I never heard about it, basically.

Mr. Birge: Fair enough. Makes sense to me. Wow, you've given me an enormous amount of information in a short time. Is there – does anything else – you mentioned that this was a project that was very memorable for you. Is there anything else that struck you about this project that was really unique or really challenging for you?

Respondent: Personally for my job I had to delve into some technical areas I hadn't got into before, so I was in a very nurturing environment there where I got to get mentored quite a bit, so just in general, it was memorable just kind of like a career point in the – you know, working with a very

cohesive team, it was very supportive, it was a memorable experience just for the fact that my learning curve kind of shot up at that point.

Mr. Birge: (Laughter)

Respondent: So it was nice to have that kind of support while that happens, you know, where a certain someone knew what I was working on.

Mr. Birge: Very cool.

Respondent: So, there were some unusual things within the industry that happen now that people were open about information. I haven't found it seem in other industries. There was a lot more shared information that was very nice.

Mr. Birge: Well, thank you so much for your time today and I'm glad we were able to finish up early and give you some of your time back. You have my email address. If you have any other thoughts that you want to share about this particular project, by all means send it along. I'd be glad to include them in my data set here.

Respondent: Okay. Sure, well good luck with the _____ I hope it goes well.

Mr. Birge: Thank you so much. Take care, now.

Respondent: Yes, thanks.

Mr. Birge: Bye, bye.

Transcriber Certification

I, Lee Baxter, hereby certify that the enclosed transcript prepared by me is a full, true and correct transcription of the Recording 110-40801 provided by Colin Birge. I further certify that I have no interest in the outcome of the project.

Entered this _____ day of _____, 2013.

Lee Baxter

15832 NE Leary Way

Redmond, Washington 98052-4329

206-650-7640

INTERVIEW TRANSCRIPT

Tape No. 110-40601

Interviewer

Colin Birge

Mr. Birge: Basically, to give you a quick idea, this is going to be about a 30-minute interview, or so, and I have a set of scripted information that I should read off, so if you'll bear with me.

Respondent: No problem

Mr. Birge: Welcome. Thanks for agreeing to participate in my in my study on designing user interfaces. I have a few questions about the design process, drawing on your professional experience. The interview should take 30 to 45 minutes. As you know, in order to make sure I get an accurate record of the interview, it is being recorded. Your name and contact information aren't included with the recording or with the resulting transcription; it is only accessible to me and is discarded at the end of the study. At any time, feel free to stop the interview and if you need a personal break, please let me know that, too.

Very important: While we will be talking about your experiences in the design profession, please, please, do not tell me anything that is considered confidential or under any non-disclosure agreements. I do not want to know.

Before we begin – start with the questions – do you have any questions for me?

Respondent: Nope. I don't think so. I don't actually remember how I answered your survey.

Mr. Birge: That's totally understandable.

Respondent: I'm not the only one that filled it out and then totally forgot about it?

Mr. Birge: It was months ago; I'd be amazed if you did remember. Let me give you some prompts. When you filled out the survey, I asked you to think about a single memorable project that required you to gather or store user information. Now, when you talked about was an issue where in you were coming up with a method of encryption of data that would be secure without being onerous on the system that used the data for processing, so this was storage of credit card information for charges and reimbursements that caused you to review some methods you were using and encryption of that data storage. Do you remember the project you were thinking of?

Respondent: Yup.

Mr. Birge: That help? So what'd I like to do in the next few minutes is just spend some time talking in detail about the way that you and your team approached that project design. Let's start with some background. In your survey, you said that this is enterprise software and services for health insurance companies, is that correct?

Respondent: That's correct.

Mr. Birge: Okay. How did this particular project get started?

Respondent: It was a requirement that came from a new government regulation so the way the software we provide to the marketplace is – it runs the back-end services for the health insurance Blue Cross Blue Shield jurisdiction is one example, not actually a customer function. They would purchase software that manages their membership data, their provider data, their provider contract, plans and products that they sell to the marketplace, either individually or to employer groups, and then all of that information goes together to manage the data associated with health insurance .

Mr. Birge: Okay.

Respondent: So, there is back-end data, and there is also transactional data. The transactional data involves claims, so when you go to the doctor, the claim goes to your insurance company. The claim has on it your member information and the provider who provided the services, the services that were provided . . . .

Mr. Birge: Right.

Respondent: It goes into what's called an adjudication engine. That engine collects all the configuration data from the system that says how the provider contracts with the health plan, what plan or product you're currently involved in, the service, whether that service is covered, if it is covered – at what percentage is it covered, etc., etc., etc.

Mr. Birge: Got it, okay.

Respondent: – and the result of that adjudicating the claim is an approval statement. It is not actually the payment. That goes into the accounting system, and then what happens is those approved for payment are sort of collected together and they get processed –

Mr. Birge: Got it.

Respondent: – the same way the claims get processed. So most of the information comes in electronically in our world today so the doctor or practice management systems or the hospital systems collect all the claim experience for the visits that were made for this day and that gets transmitted electronically to what's called a clearing house. That clearing house then patches it all together and then sends it to the specific insurance companies. It comes in as a data feed and goes into the engine, does it's stuff, and then if you want to know why you didn't get a check, customer service needs to be able to see all of that information plus the explanation of claim payment was.

Mr. Birge: Sure.

Respondent: Part of the output is correspondence with the member to say this is what we're paying or this is what we're not paying. Correspondence to the provider and also, eventually, a payment. With the new health insurance plans that are available today, there are debit cards involved because, usually it's for flexible spending accounts.

Mr. Birge: Okay.

Respondent: So if you have a flexible spending account that provides through a – through the employer – many of the administrators of the flexible spending accounts are not issuing debit cards, and the amount of money you contribute to your flexible health spending account is the available balance on the debit card –

Mr. Birge: Interesting. Okay.

Respondent: – and you would use your debit card when you go to the pharmacy or for your co-pay at the doctor's office so any approved medical expenses, you could use the debit card to take the money directly out of your account because it is your money.

Mr. Birge: Right.

Respondent: So you'd have another card that isn't an insurance card but is a debit card in your wallet so when that – the debit cards have been around for awhile, the storage of the debit cards have been around for awhile. There's also facilities for doing ESPs, or basically, transfers. Money transfers from the insurance company directly to the bank account.

Mr. Birge: Uh-huh.

Respondent: What changed, though, is the government regulations of how that data is stored and handled in the back-end systems in order to make it secure and less able to be accessed by people who shouldn't have it. So when my company – there's a variety of input for what we need to do to enhance the system, so customers can request enhancements. They can say, you know, I really need this

field to run this _____ , or I need another payment method because they dreamed up some new contracting method with providers that we need to support –

Mr. Birge: Uh-huh.

Respondent: – so a customer can come with a requirement and they give us the details of the requirement, we evaluate it and determine if willing to obtain it. If we are, if we do a high-level design and send a quote back to the customer –

Mr. Birge: Okay.

Respondent: – and they'll say whether they're going to pay for it or not. We get it from our product management group that keeps in touch with market drivers, that we need, you know, this feature or this plan type or this thing is coming up and it is, you know, well-discussed within the workplace so instead of doing work-arounds, you know, we need to meet this requirement in the marketplace.

Mr. Birge: Sure.

Respondent: In that case, it is internal development money that handles that, so you know, there's a certain amount of money allocated for investment in the product, and they put everything on the table that they need to roll up the market thing that they want, and we figure out how much it will cost to do it, how much money we will be willing to spend in our development budget, and then things follow, and the last thing we have are regulatory requirements; the things that come from federal and state governmental agencies where the government says you must do this in order to operate –

Mr. Birge: Yup.

Respondent: – those are 'must haves' and we do our best to put those enhancements into the system well in advance of the regulatory deadlines so that our customers can accept that enhancement and upgrade their system before the regulation deadlines hit.

Mr. Birge: Uh-huh.

Respondent: So, the encryption – adding encryption to the storage and view and handling of the data was regulatory – I know that was a long way of getting where I needed to get…

Mr. Birge: No, no. That was extremely helpful. Thank you.

So, let me make sure that I've covered all of this: There are – the market drivers essentially are that both market drivers internal and development drivers and also these regulatory requirements, and this particular one was a regulatory requirement. Excuse me, and it basically involved making sure that you are – were compliant with these requirements for the security of the financial transactions going back and forth, right?

Respondent: Right.

Mr. Birge: Perfect.

So, with all of that in mind, tell me a little bit about the team that helps define this design – define how you are going to respond to this requirement. Who is involved?

Respondent: Our product management group –

Mr. Birge: Okay.

Respondent: – is a group of individuals who are subject-matter experts in insurance software space.

Mr. Birge: Okay.

Respondent: They keep attuned to the direction the industry is going – they're business users, for the most part, but more super users. So they're really out – our primary customers from the design side because they get us the requirements and have to negotiate the way that we can meet those requirements with product management.

Mr. Birge: Got it. Got it.

Respondent: So product management brings the industry requirements and regulatory requirements and they also get involved in customer requirements based on – between the customer and ourselves.

Mr. Birge: Okay.

Respondent: Ourselves, meaning the development team.

Mr. Birge: Okay.

Respondent: In this specific case--my company offers a variety of products to the marketplace that meet different parts of the functional requirements of the insurance companies. Insurance companies are actually very broad-based and they do everything from specialty packages for peak insurance to, you know, very broad-based and government programs.

Mr. Birge: Sure.

Respondent: So, in some insurance companies will have home-grown systems for handling some parts of their business, like customer service or medical management, so like chronic disease. There's a few people who manage interaction with health care in order to manage chronic disease like asthma, high blood-pressure, or diabetes . . .

Mr. Birge: Sure.

Respondent: So, the management of that is that there's a lot of data and tracking, experience rating that goes in and many times they'll offer you discounts off of premiums or enhanced benefits if you do everything the way they want you to because it reduces the costs of healthcare in the long run –

Mr. Birge: Right.

Respondent: – which means that your claims are lower, so managing that often has a separate software solution because it's not just claims. There's a whole separate thing.

Mr. Birge: Got it.

Respondent: We offer add-on software that does that, but not all of our customers use it.

Mr. Birge: Okay.

Respondent: Okay? So there's a variety of module components that my company offers and the suite of components or modules for customer care, so this is the long way of saying we have the software design and construction divided between our architectural and common components and business applications, okay? So I work on the architectural and common components.

Mr. Birge: Got it.

Respondent: So, involved in this specific design project were designers for the business applications that needed to meet the regulatory requirements along with myself who was the designer for the architectural components.

Mr. Birge: Sure.

Respondent: We also had representatives from development and engineering participating in the process, and again that was for the business application as well as the architecture.

Mr. Birge: Got it. It all makes perfect sense.

At what point in the process did you get brought in on this project?

Respondent: Probably a little later than we should have.

Mr. Birge: (Laughter) Okay.

Respondent: The requirements were – part of this came about because it was a regulatory requirement but we were also building a connection and interface to a system that handles bank transactions –

Mr. Birge: Um-hmm.

Respondent: – so they would become a preferred member, and the design work for that interface was well on its way when the regulatory requirements came down, so we had to, you know, basically kind of stop and think that if they had this regulatory requirement impact what the interface was doing –

Mr. Birge: Sure.

Respondent: – then the best solution would be a common component for, and you know, architectural plug-in to handle the encryption the data security–

Mr. Birge: Uh-huh.

Respondent: – and they brought us in so we didn't need to be involved before that, but had the regulatory requirements been known earlier, then it might have made a difference.

Mr. Birge: Got it. It's part of the joy of regulation.

What's the – how many design iterations did you end up going through?

Respondent: At that point we were pretty much in, you know, sort of a waterfall process –

Mr. Birge: Got it, okay.

Respondent: – you know, instead of a you know, a structured, iterative, or agile process.

Mr. Birge: Sure.

Respondent: That being said, we had a series of meetings where we refined the design. We got together with all of the stakeholders, understood what the requirements were, kicked around possible solutions for the requirements, then architecture went off on our own side and we did research into how we could meet the requirements from a technology perspective and how we could build a pluggable component because we had different technologies involved in our software suite –

Mr. Birge: Yup.

Respondent: – so we've got web applications., C++ applications. Some things would be interfacing with databases, things that would be accessing direct data feeds, and a variety of other things so we needed to make sure we designed a solution that would meet all of the different parts that were going to be touched by this and also subsequent systems that were going to need this feature.

Mr. Birge: Sure.

Respondent: So we went back and did that work. It was in conjunction with the architects for the architectural components; we would be designing the architectural components working together, then we went back to the team. We presented the preliminary design, and then there were modifications necessary, so I think probably, if we were doing a structured iterative, say, it would have probably been two to three design iterations.

Mr. Birge: Makes sense.

Respondent: And then, coding-wise, there was a prototype, what we called a working model, which is code that can be used by another system –

Mr. Birge: Yes.

Respondent: Another one of our internal systems, that it isn't completely done yet, and then we had the temperature code, so really three development iterations and design iterations –

Mr. Birge: That makes sense.

How did – I'm getting into the details a little bit – how did the decision-making process for the waterfall design work for you? In other words, when you were faced with particular design decisions that needed to be made, you had this group of people in the room, you were kicking around ideas. How did one idea or another get selected?

Respondent: It was really a process of elimination. Somebody would present an idea and we'd entertain that until it was struck down or modified because of, you know, the needs of what we were doing. So, one example is – the actual requirement was to encrypt the data at risk, right? So, somebody enters a – well, we have a debit card –

Mr. Birge: Sure.

Respondent: – if the number is known to the person entering it, by the time it leaves the user's fingers and when it gets stored in the data base, it gets encrypted in a way that is no longer recognizable or easily connected. Okay?

Mr. Birge: Okay.

Respondent: So, we were encrypting the data at risk in just one field, not the entire record. Encrypting the entire record would introduce significant negative performance complications. Basically, it would make the server slow as molasses–

Mr. Birge: Makes sense.

Respondent: – so, that wasn't an option. We did discuss, you know, basically encrypting the whole record and that was just, you know, even though the security people wanted us to do that, that was just not a viable solution.

Mr. Birge: Sure.

Respondent: So, the method of encryption was really up to the design and architecture, you know, the common components team, to determine what specific method of encryption we could use within the industry that would meet the regulatory requirements and, you know, the deliver mechanism. You know, we didn't want to write our own encryption method. So the fine-tuning of the design came in to – we understand that it has to be encrypted when it is written but at what point do you unencrypt it? Do we send it to the external system or the banking system encrypted or along with the key and then they unencrypt it? So, do we give them a copy of our component and we give them the data plus a key and they use it to unlock the value? Or do we de-crypt it – unencrypt it – and then ship it? I mean, that seems like a simple decision, but that was probably one of the most time-consuming decisions we had –

Mr. Birge: The threat model, alone, I would imagine.

Respondent: Well, yes. And then you have to evaluate how to secure the transaction. Can you assume that the transaction, itself, is secured –

Mr. Birge: Right.

Respondent: – you know, and if it is, then sending it unencrypted is not a problem. So who were we really protecting at that point –

Mr. Birge: Sure.

Respondent: – so how did the decision-making happen? Then we proposed the solution and basically worked together to shoot holes in it so, you know, concerns will be voiced. We either refine the design to answer concerns or we had them moved to another design.

Mr. Birge: Right. Makes sense to me.

Does the user have any visibility into any of this?

Respondent: – so the user, in this case, there were a number of user touch-points –

Mr. Birge: Sure.

Respondent: – in our system, one of the users is other systems, so when you write use case, it's not just somebody sitting down and doing work on a computer, it can be another system getting the data –

Mr. Birge: Totally.

Respondent: – so that's--- one of the users of the system with the enhancement was going to be the banking system, so they definitely – their requirements had to have a seat at the table because we couldn't add overhead to them, because then they wouldn't want to be our preferred vendor.

Mr. Birge: Right.

Respondent: They would say this is going to cost too much money to do this. So, we had to take more of this on ourselves, so that was one of the users at the table. We had the use of the entering the debit card information the first time –

Mr. Birge: Uh-huh.

Respondent: – in the customer service manager module. The debit card can also be entered by individuals through a web portal.

Mr. Birge: Uh-huh.

Respondent: The web portal is controlled by the customer but the services that managed the data are controlled by us.

Mr. Birge: Got it.

Respondent: And the core interface elements—because the look and feel are controlled by the customer but the core interface elements are provided by us and then they modify for the customer or the client. So we needed to make sure that the web interface was – was accommodated in real time, and we also needed to accommodate the requirements of customer service, reporting and letter generation. This data is shown on the screen, so what will it show when encrypted? How do I meet that need? So I can't just – so the customer service user, we needed to determine what their requirements were for those different users of the data, whether it was entering the data, reviewing the data, or transacting with the data. So what's the minimum information that we can show them and is there any way we can do that? Of course we want to minimize the database changes to keep the cost of meeting the requirement as low as possible.

Mr. Birge: Right.

How did you go about – was there anything unique about the process of getting all of those user requirements together and understanding how they all worked together?

Respondent: What's the question . . . Were there any challenges?

Mr. Birge: Yes, what were the challenges that were involved?

Respondent: This is probably not an uncommon challenge; the technologists have a habit of thinking only of the system –

Mr. Birge: Um-hmm.

Respondent: – and the gracefulness of the technical solution, and not necessarily how that is impacting the user. So, one of the things that I needed to do along with the designer from the business application was remind the architect and the people doing services that we needed to provide sufficient

details about the data that they couldn't see to get them in the security so that the data was actually there, in fact.

Mr. Birge: Sure.

Respondent: That make sense? They enter something and they save it and it goes away. That's not going to-- .(laughter)

Mr. Birge: Understood.

Respondent: So, that was probably the primary challenge. Most of our users, for the most part, are – the customer service users, we have a very good feeling for. We have a customer service user group –

Mr. Birge: Uh-huh.

Respondent: – that we communicate with regularly and they give us enhancements for that area of the system, so the business application designer was in touch with the customer liaison and very familiar with the services represented so we made sure that that user community was well-represented in the design phase. And then the system-to-system communication was much more straightforward, because you didn't have to really talk to anybody.

Mr. Birge: Sure.

Respondent: We had to make sure that we didn't add, as I said before, onerous requirements on adopting systems, so, you know, it needed to be a lightweight solution that we handled and managed so that it could be transparent to anybody that wishes to view it on the outside. So, it was – I guess one of the specific challenges was this, was balancing that user – the user needs to be secure that the data is there and that it's correct when they can't see it and we're not going to show it to them, and we needed to do the whole thing in a way that would not negatively impact system performance, or require too many changes to the parts of the system that were already in place, so we needed to be able to transport the

data, whether it was encrypted or unencrypted, in the fashion that we were already transporting it, not asking to give new technology communicating that data to the web.

Mr. Birge: Got it.

Respondent: There were a whole bunch of things it couldn't do. It needed to be transparent to everybody with access to the data base.

Mr. Birge: Understood. Writing something down. Sorry.

Did – at the end of the day, were you satisfied with the design . . . do you think it came out the way you wanted it to?

Respondent: It would have been nice if it were a little bit more graceful, you know, but with the constraints that we had, it was okay.

Mr. Birge: When you say "graceful" what are you thinking of there?

Respondent: Well, because I work on the architectural part of the system, you want everything to be as clean and pristine as possible, so if you're – it should be five lines of code instead of 500 lines of code at that level.

Mr. Birge: Sure.

Respondent: The simpler and more straightforward the solution is, the easier it is to make it transparent to other systems, and the easier it is to plug it in with other things. If you have something with a lot of arms and legs – conditional – it gets very complicated. So one of the – one of the unfortunate parts of it was we actually got probably seventy-five percent of the way through the construction phase and we discovered that we couldn't use the encryption method that we had picked –

Mr. Birge: Oh, no!

Respondent: – according to current industry standards. We didn't really change our methodology, but the reason we couldn't use it was because it would sell to the international marketplace.

Mr. Birge: Uh-huh.

Respondent: And the encryption method that was currently preferred in the United States is actually protected under government secrets, probably the wrong thing, but basically, you can't export it.

Mr. Birge: Okay.

Respondent: So, we couldn't go out the door with the solution that we first wanted, because we couldn't export it and therefore we would need an alternate solution for international customers, which was just not an acceptable or workable solution, so you know, we sort of keep our eyes on it, waiting for something to change and go back and look at it.

Mr. Birge: Got it.

Respondent: But we did wind up in the long run meeting all the requirements that anybody came up with –

Mr. Birge: Well, good!

Respondent: – in the time frame. It came in within budget, and, even though from a purist's perspective, it probably could have been a more graceful solution, it has been a couple of years since we've had to do anything. We must have done something right. We haven't had to fix it – we haven't had to…–

Mr. Birge: Congratulations.

Respondent: So –

Mr. Birge: Very good.

This has been enormously helpful. I'm really very grateful to you for your time. Is there anything else that you think is really unique or important about this project – anything else you want to share?

Respondent: Not that I can think of.

Mr. Birge: Okay. Fair enough.

Respondent: But if you have any more questions, please feel free to reach out again.

Mr. Birge: I appreciate that; thank you. And again, thanks for taking the time this morning. This is a real help to my study and also, hopefully, a real help to designers in the future, once we get this all written up. Thank you again. Let me know if I can answer any further questions on my side, and you do have my email, so if you think of anything else you want to add, by all means, let me know.

Respondent: All right. Will do.

Mr. Birge: Thank you so much. Take care.

Respondent: Okay. 'Bye

Mr. Birge: 'Bye.

Transcriber Certification

I, Lee Baxter, hereby certify that the enclosed transcript prepared by me is a full, true and correct transcription of the Recording 110-40601provided by Colin Birge. I further certify that I have no interest in the outcome of the project.

Entered this _____ day of _____, 2013.

Lee Baxter

15832 NE Leary Way

Redmond, Washington 98052-4329

206-650-7640

INTERVIEW TRANSCRIPT

2011-0602

Tape No. 110-40604

Interviewer

Colin Birge

Mr. Birge: . . . so, I have the usual script that I need to read. Welcome. Thank you for agreeing to participate in my study of designing user interfaces. I have a few questions about the design process drawing on your professional experience. The interview should take about a half hour. As you know, in order to make sure I get an accurate record of the interview, this is being recorded. Your name and contact information aren't included with the recording or with the resulting transcription. It is only visible to me and will be tossed at the end of the study. At any time, feel free to stop the interview. If you need a personal break, let me know that, too. Very important: While we are talking about your experiences in the design profession, if you have anything that is considered confidential or under non-disclosure agreements, please do not tell me, I don't want to know. Before we begin, do you have any questions?

Respondent: No.

Mr. Birge: Very cool.

Respondent: So human subject is happy.

Mr. Birge: . . . human subjects is happy. When you filled out a survey that was an unconscionable number of months ago, I wanted to ask you did you have _____ projects that required you to gather or store some user information and the one you mentioned was a membership data base with about three levels of access, admin, member, and public. Do you remember that?

Respondent: Um-hmm.

Mr. Birge: What I'm trying to do is –

Respondent: Thanks for reminding me.

Mr. Birge: What I'd like to do is spend some time sorting through how you approached that design, so let's start with some background. This was a database website for an academic audience. You said something about that.

Respondent: Principally an academic organization.

Mr. Birge: Okay. How did it get started?

Respondent: The organization?

Mr. Birge: Well, the project, is what I was thinking of.

Respondent: There was a project that had been done by a colleague, and the technology that supported it was dying. We needed it to be re-hosted and along the way, a variety of affordances were identified that clearly seemed to make sense because the bylaws of the organization, we had an obligation to publish a directory and it was felt that we could do that as a public access level of access, and clearly as membership coordinator and so on there was a need for a kind of administrative level that had no holds barred in terms of what was there and in between, it was felt that, partly because the earlier implementation had included it, but it was felt that it was reasonable to give the users some management control of their own visibility in order to make it visible and to whom. So, it was decided that while name

would be globally public and you can't turn it off, everything else lives in one of the other two levels of visibility –

Mr. Birge: Sure.

Respondent: – and then there was some pieces of information that aren't revealed particularly to even the individual. They have a history of membership renewals and some that are really only visible to the membership coordinator and other admin users.

Mr. Birge: Got it.

Respondent: So, a little bit of history, a little bit of deciding about it, and certainly an attempt to make a sort of standardized ideal of visibility you want.

Mr. Birge: Sure. Now when you say "standardized" are you thinking of taking –

Respondent: Maybe not "standard". "Regularized" might be a better – at least in its own context.

Mr. Birge: Got it.

Respondent: We wanted one pattern of, you know, text field construction, if you will, the function construction and the rest of that so that it wouldn't be hard to make –

Mr. Birge: Got it. Who was involved in this effort, besides yourself?

Respondent: I had a student that became interested in it after I taught a course in web technologies, and had manifested some interest in doing an independent project so I said, well, we had this organization that needs to do this thing and you could work on that as a armature to wrap your head around and then there was two or three individuals within the organization, including the author of the old system that was dying who was willing to sort of contribute, critique, and comment.

Mr. Birge: So, the two to three individuals who were stakeholders or did they have –

Respondent: No, they were sort of in and out, more or less. There were stakeholders in the organizations, but not so much stakeholders in the project, such as would benefit the organization.

Mr. Birge: Sure. So you had this prior project, or this prior piece, and someone identified the need to replace it. Was that you or was that somebody else? How did you get involved?

Respondent: I was functioning as, well, let's see – I've been deeply involved in the organization for twenty years and at the time, I think I was just coming off of a stint as president and was functioning as webmaster. I'd been principal webmaster for the organization for – since '95, with few exceptions, and so when it became clear that the whole system was going to go away, and somebody needed to step up and sort of take on making the new system and nobody else volunteered –

Mr. Birge: (laughter) Got it.

Respondent: – so I was capable and willing, especially with the design work use as a learning exercise for the student, so I said, well, we'll take this on.

Mr. Birge: So, you had this prior system. How much of the prior system were you able to re-use or to integrate into the current design?

Respondent: Not a whole lot. Literally, some of the graphics. Certainly, some of the data base structure and clearly some of the behavior. We named it Cameo 2.0, and after the original Cameo, and so on. It was meant to carry forward a certain amount of similarity. The original system had been built in an ad-hoc way. This guy who had maintained it previously. So it had a bunch of issues, hopes, starts and things in it that either didn't work perfectly or had never really seen light of day as user accessible features, including some of the registration for conferences, election support and some other stuff. We hacked out a bunch of that and threw away essentially. There was no code base to borrow, so it was just a matter of how it was meant to behave. But to know – for instance, when we did import most of the data from the old system so big chunks of what we know about. The schema for what we know about members was pretty much patterned after that.

Mr. Birge: How many design iterations did you wind up going through?

Respondent: Oh, it's still going on –

Mr. Birge: (Laughter)

Respondent: I have a to-do list of a variety of things that it needs. I don't know that they had clean boundaries. I just tend to be an incrementalist because I don't have big blocks of time to do these things sometimes. Partly because of I've seen too many projects that fail through overreaching, so once we had a functional system in place, every now and then – summer break, Christmas break – some things sort of substantial would need to be done. There have probably been – there have probably been really only four substantive, largish changes since it went live. And a smattering of bug fixes, and –

Mr. Birge: How about changes to the design that you thought of before it went live, when you were working out--

Respondent: Before I started working with a student? That was somewhat negotiated between what he could be expected to do –

Mr. Birge: Sure.

Respondent: – what we had, what I knew how to do. I have not worked with stored procedure, PHP things before. The server that we built it on at the time didn't have stored procedures whereas the original application had used some stuff that was essentially computed on the fly. So we had to – that was a technological condition that led to some adjustments or changes –

Mr. Birge: Sure.

Respondent: I usually try to engage with the stakeholders in projects like this so that there is some buy-in and reason to use it when you're done. This organization isn't, you know, wildly volunteeristic –

Respondent: (Laughter)

Respondent: Outside of conferences, you know, people – it's like pulling teeth to get them to participate in these and other kinds of things unless there's a fair amount of buzz around it, And membership data base, it doesn't feel like buzz. So how many alternative designs? It was, I imagine there

were some things that happened along the way, but pretty much – it was pretty straightforward. You know, you've got people and you've got, you know, we call them subscriptions, but you've got membership years and you have to keep track of the two. There's some extra wrinkles – a benefit of membership is access to a data base that's maintained elsewhere, so when you renew your memebership this thing has to kick out an email to them that says that you've renewed your membership. One of the substantial changes that we did go in was support for PayPal, so I had to figure out how all that stuff worked so they did test-drive it, and then roll it into the existing data base that had been driven by a membership officer, depositing checks, and then going into the data base and saying it's paid.

Mr. Birge: Got it.

Respondent: So that was a fairly substantial change, but it's an almost non-change – you fill out the membership from the same way, it's just that what happens at the end instead of writing a check you hit the PayPal button. Then you go off and – what happens to you, the user experience is substantially different. But our application was pretty well hidden, and figuring out how to actually do this. So it's like most software creep, it's accreted functions and functionality as time has gone on. Where it was once just about keeping track of and displaying this alphabetical sublists. I added-- members had interest key words. I added a wordle (?) style birds-of-a-feather kind of thing phrase, a wordle graphic driven by the prevalence of interest key words and they're tied to--so if you hit one of those words, it does a data base search on folks who used that word as one of their interests. It's an alternative way of accessing the directory, basically. It has search features so you can search for people that have dot-tamu in their email address, to see who you know at Texas A&M. That's just an accretion. Partly it was an attempt to get people to actually, again, to engage, use, put in interest key words because they would get something out of it.

Mr. Birge: Right. What was – did you do any user research in this process –

Respondent: Sure, sure – not active user research, not surveying the members and finding out what percentage would be interested in having what features, because I suspected there would be very little feedback. I'm pretty sure that I emailed the membership and said if you have anything – any suggestions about the old system that you'd like to throw away, I'd like to hear them. I don't think I got any responses.

Mr. Birge: Got it.

Respondent: And certainly, the guy did the first system – he is a friend of mine – so I shoot him an email and say we got another whack at this so take a look at it. Operating system and browser quirks I would usually sort of ask a slew of folks to just take a shot at it to see if Internet Explorer was doing anything particularly weird with rendering of things and stuff like that, periodically.

Mr. Birge: So, you mentioned talking to folks about problems or technical issues that were coming up; did you use any other resources for that, apart from sending out to friends or colleagues?

Respondent: Well, significant use of PHP and mySQL, dot net and org web sites, their formal documentation, and probably a certain amount of other stuff, and –

Mr. Birge: Such as?

Respondent: – whatever Google found, kind of other stuff.

Mr. Birge: Got it.

Respondent: I found that W3 schools to be a really strong site, but that's actually come along since this project was largely done, and so I imagine to the principal sites for most of that stuff. Just trying to figure out how to do certain kinds of data base queries and things like that. I had the book that I no longer have here that I used as a starting point at one stage to sort of get my head around how to do some of that stuff.

Mr.Birge: Do you remember the book?

Respondent: Something like "Apache PHP and mySQL in a Weekend," something like that. I have it still, at home, but I don't think I—in fact I just took it home recently, but I don't think I've referred to it in awhile. It was when we started the project. I'd done web services fine. I hadn't figured out – well, this actually has to go back to about 2004 – 2003 – when I was on sabbatical, I actually was learning some of that stuff, but I knew that this horizon was approaching on the old system and then, I taught the course, I think it was in '06 – '07 when the student did the independent study. It would have been in the spring. We sort of got serious over the summer about trying to change the what he had done. –

Mr. Birge: Got it.

Respondent: And then probably would have been about winter '08, and then Paypal came along about a year later, during –

Mr. Birge: You mentioned PayPal. What other differences are there between the version that you originally shipped and what you've got now?

Respondent: Didn't ship far (laughter), it runs here. If we can call it "shipped". Oh, there are some – there are some logic errors and bookkeeping kinds of things, say. When somebody signs out to go on a state of being unknown to a state of being known but not fully such number because the payment has not processed yet. So, they go from a null record to an applicant record. An applicant record has a date attached to it, but for instance, it turns out that if you are an applicant from more than the last year ago, it's actually won't let you renew. Because it – it's sort of implied in the logic that was built into it in places were some maintenance things that really didn't happen. So, you know, as those things crop up, they've either gotten fixed by doing the maintenance on the data or they've gotten fixed by doing maintenance on the code, changing the logic. We needed support for testing whether people were current members so I added just some really simple sorts of queries that folks running the conferences could use to-- because the members get a different registration rate, so they can test whether a given name was a known member's name. I don't think it's been particularly heavily used, but it's stuff like that. We run an

election on randomly-generated authorization codes for people to vote with so they can sign with an authorization code that comes out in the data base so we can test it against those and so on. We just finished an election and that stuff was added after the initial implementation so those things, the Paypal thing, the wordle—Some administrative features like the ability to select sub-sets of the membership and send them email has become interesting to people. It's remarkably complicated just how gnarly those kinds of selections can potentially be. One of the features we never did implement, partly out of security concerns, was the ability to take an ad hoc query and execute it and which would have allowed a savvy membership coordinator to, you know, find things that weren't built into the software, and in fact, I'm not sure that any of the membership coordinators have been that savvy that they could be trusted with SQL syntax without mangling things –

Mr. Birge: Was that a security concern?

Respondent: I was – I wasn't sure how I wanted to handle the security in it, so not being sure, it doesn't happen. And then, I've partly – it's the kind of thing that can be a really big lump of code to make happen and it wasn't clear to me how necessary it was, so there are some, you know, sort of every now and then something that need to be done will show up, like finding library numbers from out of the data base as opposed to regular members, because they pay more for their membership. We need to be able to identify them and they really ought to be – really you list members alphabetically, so listing, you know, Washington, according to the librarian doesn't make a lot of sense. But on the other hand, listing all the universities under 'u' doesn't make a lot of sense, either, so there's something to be said for information just straight up; how do you do these things kind of raise their head every now and then. Some of them have been answered and some of them haven't.

Mr. Birge: What kind of user information do you collect in the membership data bases besides the names?

Respondent: Well, they are asked to provide their name and address, phone number, an email address. The email address is essentially their user name. That's necessary, but in addition to that they get a first and last name and, you know, an appellation – Mr. Prof., Dr., whatever – an affiliation, interest keywords, a personal website URL, phone number, fax number, I could go look if you want the full list, but you know, it's that kind of stuff.

Mr. Birge: Fair enough.

Respondent: and the membership record is basically when they – when they did it, when it expires. Does it expire December 31? So that's kind of a preset, and what, how they register for the student, faculty, I mean, regular, library, and so on, and what they paid.

Mr. Birge: Were there any concerns that arose when you were thinking about how to code the information?

Respondent: Revealing? Accidentally? Yes, in the sense that there was efforts made in the coding not to make it fragile to SQL injection.

Mr. Birge: Sure.

Respondent: No, in the sense that membership was pretty well signed off on this stuff previously, and no in the sense that members could individually choose to not reveal to the membership, assuming that the code all works, all – everything, except their name. We did anguish over defaults for awhile – whether you default to public, default to members only, default to private, because people are famously sluggardly about updating and changing things. I believe as it stands now, it defaults to members only. Which was a push towards making information more available., you know, making it – oh, and one of the other things we gathered is, we asked for a head shot. It was optional, but they could upload an image. So the goal is, at least in part, some social support.

Mr. Birge: When you were trying to determine the defaults, how did you end up coming to that decision; was that –

Respondent: Partly thinking about it; discussions with other folks who were – would respond to theories within the administrative arm of the organization, and then I tend to be fairly careful to document when announcing stuff to say to the membership, there's a million "ifs" but to say this is what we're doing. If you don't like it you should get in there and change your exposure to – you have to act, in the great existential dilemma, you have to act as something, and the next best thing to being guilty of mis-stepping is to, you know, act invisibly is worse, actually, so when we've done stuff that might potentially bother people in terms of privacy, is tell them about it. And you know, for instance, the head shots that we've put up, we're all initially head shots had been in the other system. They had to upload those, so I took that as a tacit permission to reveal them and I would not take a picture that I might have and find someplace and stick it into the data base without them having some say or choice, whatever, in the access.

Mr. Birge: Makes sense. Okay, anything else unique or interesting about this design in particular in your mind?

Respondent: Well, there's a challenge that exists. The organization has a public website and there's an integration challenge. When I designed the public website, at one point I had a proposal for a sort of log-in to the membership window within the public page as an icon, and we eventually scrubbed that, partly because it wasn't real clear what you would display there. It was sort of like when you're doing membership stuff, you're doing membership stuff, and not browsing the public site, and partly because I think it was felt that the predominant visitor would be not a member and that we were giving up too much screen real estate to essentially member-centric stuff, so the link from the public site to the membership system was buried down one level.

Mr. Birge: Right.

Respondent: So, then, you know, boundaries: the sort of general designing question is how do you integrate and find boundaries and so on, so those are the things for which only members have access

other than information about other members, so there's the directory function, and then there's access to this third-party data base of papers –

Mr. Birge: Sure.

Respondent: – and we provided a facilitation mechanism within the membership data base that says if you're a brand member and you just told us your name and affiliation, we can fill in that for you on their form, but you have to take this link to do it, right, so then once it's been filled in and presumably submitted, we can't tell because there's no call-back mechanism. Then we can send the membership confirmation so there's a two step – there's a little block of service links that then, when the election is running, that's where the election code shows up and when what else pops up there? There's a link to another online data resource that's a members only thing so you don't get at that stuff unless you come in to the membership data base.

Mr. Birge: Got it.

Respondent: I'd say essentially support for a variety of member services, this is not so much member data base but it's tied to membership so it lives within the usual framework of the membership data base, and there is, in fact right now, a group which is working on a substantial overhaul of the organization's web presence and I'm not a part of that. They have ideas about what they want to do and how it's going to work and it's probably going to be really way cool and if people will participate in that one where they haven't participated in the existing system, and I'll believe it when I see it.

Mr. Birge: (Laughter)

Respondent: I don't think the culture is quite there. It's susceptible to change, and this organization is just not a particularly chatty organization. The membership is pretty much moribund except for position announcements and calls for proposals periodically, and there are other organizations that I'm also on the mailing list that are must more eager actors within the membership. It's just an intriguing question whether there are any collection of affordances you can provide on a website that can

make that happen. I think it's deeper in the culture than that, so – so, we'll see. I wish them luck since their going to commission a bunch of stuff that I can't. I don't know whether they have eyes on the members or not, but they're going to pay big bucks for this, whereas everything we did was voluntary, and –

Mr. Birge: This has been enormously helpful.

Transcriber Certification

I, Lee Baxter, hereby certify that the enclosed transcript prepared by me is a full, true and correct transcription of the Recording 110-4060X provided by Colin Birge. I further certify that I have no interest in the outcome of the project.

Entered this _____ day of _____, 2013.

Lee Baxter

15832 NE Leary Way

Redmond, Washington 98052-4329

206-650-7640

Colophon

This dissertation was drafted on a MacBook Pro using Scrivener 2.3.1 (http://www.literatureandlatte.com/scrivener.php) by Literature & Latte. Tables and graphs were created using Microsoft Excel for Mac 2011 and OmniGraffle Professional 5.4.2. Citations were added using EndNote X6. Final layout, creation of the index & table of contents, and other document design were performed in Microsoft Word for Mac 2011. The completed dissertation was published in Portable Document Format (PDF).

The font used in this dissertation is Palatino Linotype. Headings use Garamond bold fonts.