Privacy and Security in the Brave New World: The Use of Multiple Mental Models

Sandra Spickard Prettyman[1], Susanne Furman[2(✉)], Mary Theofanos[2], and Brian Stanton[2]

[1] Culture Catalyst, 113 N Democratic St., Tecumseh, MI 49286, USA
Sspretty50@icloud.com
[2] National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, USA
{Susanne.Furman,Mary.Theofanos,Brian.Stanton}@nist.gov

Abstract. We live in a world where the flow of electronic information and communication has become a ubiquitous part of our everyday life. While our lives are enhanced in many ways, we also experience a myriad of challenges especially to our privacy and security. Survey data shows that the majority of people are 'very concerned' about privacy and security but that they don't always act in ways to protect their privacy. Our goal was to explore how participants understand and experience privacy and security as they engage in online activities. To that end we used a qualitative approach to understand the participants' mental models of online privacy and security. The data from our 40 interviews show that users have multiple mental models that guide their understanding of and experience with privacy and security. These mental models not only operate simultaneously but are rarely fully formed and often contradict each other.

Keywords: Mental models · Online privacy and security · Qualitative approach

1 Introduction

Today there is no such thing as privacy. It looks like privacy and it feels like privacy, but there is no such thing as privacy. I look at what the government could do if they wanted to, so there is no such thing as privacy. (*Patience, Female, Age: 40 to 49*).

We live in a world where the flow of electronic information and communication has become a ubiquitous part of everyday life and embedded in our interactions in and expectations of the world. This technology enhances our lives in many ways, but also comes with its share of challenges especially to our privacy and security. These challenges have become more complex as the devices we use to access and utilize information and communication systems have become more mobile, varied, and used more frequently. With the shift to doing more of our banking, shopping, and communicating with intricately linked and networked systems comes an increased concern about the privacy exposure and security of our personal information. Often these concerns are misunderstood or ignored. In this context, cybersecurity training and education are imperative if end-users are going to navigate the online environment safely and effectively. However,

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 260–270, 2015.
DOI: 10.1007/978-3-319-20376-8_24

in order to design effective cybersecurity training and education, we must understand how people think about and experience online privacy and security in their everyday lives. Many researchers in computer and online privacy today argue we need continued research to gain a better understanding of end-user beliefs about, experiences with, and desires for mechanisms to protect privacy and security [1–4].

This study presents findings from a qualitative inquiry into people's understanding of and experiences with online and computer privacy and security. Our goal was to explore how participants understand and experience privacy and security as they engage in online and computer actions and activities in their everyday lives and to determine if a mental model helps them navigate these interactions. Participants in the study articulated a belief that they were living in what we call a Brave New World, one in which privacy is a thing of the past and security is a "blanket with holes in it" (*Patience, Female, Age: 40 to 49*). In this brave new world, people do not draw on a single mental model, rather they use multiple mental models, often at the same time, that are often only partially- (or ill-) formed. Understanding these models and how people utilize them can help us develop and design better approaches to education about cybersecurity for all users.

2 Background: Mental Models, Privacy, and Security

"A mental model is a simplified internal concept of how something works in the real world" (p. 1) [5]. We use mental models to help us decide the best course of action in given or unfamiliar situations. Since the 1990's, mental models have been used to try to understand human-computer interaction, and more recently have been used to explore cybersecurity and risk communication. Camp presents five different mental models that can be used in risk communication to users: physical security, medical infections, criminal behavior, economics failure, and warfare [6]. Subsequent research built on Camp's work found sharp differences in the mental models used by experts and non-experts as they considered security risks [7]. Wash describes two major categories of "folk models" utilized by non-expert participants, finding four models within each category of malicious software and malicious computer users [4]. What links all of this work is that we must first grasp how users understand and experience online and computer privacy and security in order to help protect individuals and institutions.

Privacy is a concept that is highly contextual and often contested, with little agreement in the literature regarding how to define it [3, 8]. Brandeis and Warren asserted that privacy is the right to be left alone, which has influenced privacy legislation in the United States for most of the 20th century [9]. More recent definitions of privacy recognize that a person's privacy depends on the extent to which others have access to information about them [10] or about the degree to which we have control over information about ourselves and our environments [11]. The one constant in the privacy debate is that surveys show the majority of people are 'very concerned' about their privacy [12]. Yet empirical evidence suggests that there is a significant discrepancy between privacy principles and privacy practices [3]. While people articulate a concern for their online privacy, they do not always act in ways to protect it.

This discrepancy may result because users generally view privacy as a social concern and security as a technical concern—something that can be deployed for the purposes of protecting privacy. Dourish and Anderson define security as "the state of being free from danger" (p. 322) [1]. They frame online privacy and security as "collective information practices - the ways in which we collectively share, withhold, manage information and interpret these acts and deploy them in everyday social interactions (p. 335)." In this study, we situate privacy and security as collective information practices.

As researchers, we come at this work from very different disciplines, both academic (i.e., engineering, psychology, sociology, computer science) and methodological (i.e., both quantitative and qualitative); something which we believe helps us "to bridge intellectual traditions" [13] and provide a more holistic understanding of the issues under investigation. The National Research Council (NRC) has argued for more research to be conducted using an interdisciplinary approach [14]. This work responds to that call and seeks to broaden the scope of work found in usability and cybersecurity.

3 Methodological Approach

Given the exploratory and descriptive nature of this work we chose to use a qualitative approach for the study. Our research questions for the study were the following:

1. How do participants describe their experiences with online privacy and/or security?
2. What, if any, perceptions do participants have regarding online privacy and/or security?
3. How, if at all, do participants use mental models as they think about privacy and/or security in the online environment?

We conducted semi-structured interviews with 40 participants and used a recursive analytic process as we worked to make sense of the data. The semi-structured interviews provided us with similar data across the interview participants, allowed for flexibility and the ability to follow participants' leads during the interviews; and provided for structures for coding and analysis and helped us develop analytic accounts rooted in the data. We were interested in how users understand and experience online privacy and security. We were not interested in what larger numbers could tell us statistically, but rather as Schoeman advocates, in the rich and detailed data that our participants could provide [10]. Our goal is to tell the story of online and computer privacy and security from the perspectives and through the words of our participants.

3.1 Sites/Participants

Researchers from the National Institute of Standards and Technology (NIST) recruited participants in the Washington, DC metropolitan area using email and in central Pennsylvania via an advertisement in a local newspaper asking for participation in a NIST study about people's perceptions of online and computer security. They were told that they would participate in a one-hour interview and compensated $50 for their participation with requirements of having an active email address and being 21 years of age

or older. Our goal was to have participants from different backgrounds (age, gender, geographic location, employment) and who had a wide range of and experiences with computers.

We interviewed a total of 40 participants for the study, 27 from the metropolitan Washington DC area and 13 from central Pennsylvania giving us a sample from urban, rural, and suburban settings. Throughout this paper, we use pseudonyms when referring to participant statements. There were 21 women and 19 men who ranged in age from 21 to 79. All but two participants had some college education and six held advanced degrees; only one of the participants worked in the technology industry (but not in the realm of privacy and security). Participants were asked to evaluate their level of computer knowledge: 12 (30 %) reported little knowledge; 24 (60 %) reported moderate knowledge; 4 (10 %) reported expert knowledge.

3.2 Data Collection and Analysis

Data collection occurred from January to March 2011. The semi-structured interview protocol included: demographic questions; information about online activities, behaviors, and knowledge; familiarity with security terms and icons; and beliefs and perceptions about computer and online privacy and security. The protocol was designed to elicit data about participants' beliefs, perceptions, and behaviors related to online privacy and security. Once all interviews were completed, a NIST researcher in the project transcribed them, along with any field notes related to them. Initially, quantitative analysis was conducted on the data collected from the interviews [12].

Subsequently, we conducted qualitative data analysis with multiple readings of the full data set by all researchers in the project, followed by individual and group coding sessions. The group constructed and operationalized an initial a priori code list that was based on the literature and on our own knowledge as researchers in the field. We used an iterative process of: working with a subset of four interviews each to determine inter-coder reliability; discussing codes, definitions, and issues using them; refining our use of codes until we reached agreement; operationalizing emergent codes and solidifying our understanding of our new code list. At least two researchers coded each of the remaining interviews. The goal was to insure that the use of codes and their application to segments of text was consistent amongst the researchers; "the more coders (using the same codebook) agree on the coding of a text, the more we can consider the codebook a reliable instrument (i.e., one that facilitates inter-coder reliability)" (p. 310) [16].

4 Results

Previous research argues that a mental model guides people's behavior related to online and computer privacy and security [6, 7, 17]. While different mental models are described in the literature, the implicit understanding is that people use one as they work to make sense of and make decisions about online privacy and security. Our data shows that there are multiple mental models that operate, often simultaneously as users experience privacy and security in this brave new world. These mental models are rarely

fully formed, but rather only partially formed, and they often contradict each other. In the sections below, we describe the ways in which participants draw on a variety of multiple mental models as they discuss their understandings of privacy and security.

4.1 Living in the Brave New World: The Need for Multiple Mental Models

In 1965, Gordon Moore conjectured that the number of transistors that could fit on a square inch of silicon would double every year, leading to exponential shifts in our devices and their capabilities [17]. "[T]he impact of "Moore's Law" has led users and consumers to come to expect a continuous stream of faster, better, and cheaper high-technology products" [18]. The pace, types, and consequences of interaction have all changed—leading to a Brave New World where participants attempt to navigate, often without adequate tools or training. A world where a single mental model may limit their ability to adapt to change but where the use of multiple mental models may help users cope in this rapidly changing technological landscape. As Lewis *(Male, Age: 50 to 59*) explained, "Things have moved so fast. There is so much information out there about everyone…I trust if my credit card or bank info is stolen that my bank will take over."

4.2 Life in the Brave New World and a Desire for the 'Good Old Days'

Many participants talked about the world today as if it were a very different place than it had been. A world many of them would like to opt out of, but believe they do not have the ability to do so, and where their experiences with privacy and security lead them to long for the 'good old days' where they felt safer and more comfortable. As Cindy (*Female, Age: 20 to 29*) explained, "…it [Facebook[1]] is like the Hotel California – you can check out but you can never leave. Once they have your email address and your name – you are out there forever….Our information is all over the place. I would prefer to go back to paper mailing and close out all of my [online] accounts."

Tiffany (*Female, Age: 20 to 29*) said: "My friends make fun of me and call me an old person. I know people say things about how people can just open your mail, but I feel safer. I feel vulnerable when I have to enter my bank routing number and checking number somewhere online. It gives me piece of mind when I write a check and I put it in the envelope and send it off. The comfort comes just from that." Edgar (*Male, Age: 40 to 49*) explained: "I don't pay bills online. I don't trust it – I feel like I have no control if something happens. I would rather call and pay it over the phone. I feel like that is more secure than having all that information situated on the Internet where all these things get done automatically." Kendall (*Female, Age: 20 to 29*) explained: "I don't pay bills online. I feel it is much better to put it in the mail and I feel the mail is pretty secure. I know that people can get viruses and I don't know how much of that is stored on the computer. I feel safer and they don't have access to my information." Norma (*Female, Age: 40 to 49*) said:

[1] Disclaimer: Any mention of commercial products is for information only; such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best for the purpose.

"I think computers can be dangerous because it gives the information out so quickly. It is not like word of mouth or spreading something to a neighbor or coworkers even. If it is something on a computer then everyone can see it within a second. There is no privacy at all." Murray (*Male, Age: 40 to 49*) explained: "For me, the disadvantage [social networking] is that we have become an impersonal society. For me, I want to hear your voice. People don't even have the courtesy to pick up the phone anymore."

Interestingly, not only the older but also the younger participants wanted to return to the good old days, back to what they perceived as a simpler, safer time. Most lacked a fully formed mental model to guide their thinking about online privacy and security and this may have led them to believe things were better and safer in the past. Without this fully formed mental model they often felt uncomfortable and unsafe.

A few participants did talk about the brave new world as the norm: "Well, it is 2011 and I am 24 – so I never thought about that – the other way was before my time [speaking of online bill paying]." (*Rod, Male, Age: 21 to 29*); "I don't know why we instant message (IM) – sometimes I will IM a friend who lives 10 min away and I don't know why I just don't talk to him. And he likes to talk that way more than he does on the phone." (*Jessie, Female, Age: 40 to 49*); "I licked an envelope the other day and I thought wow this is odd." (*Michelle, Female, Age: 40 to 49*).

For Rod, Jessie, and Michelle, new technologies were part of how the world works, something they did not even think about as they engaged in their daily activities. While they are accepted, most participants are still suspect of new technologies and their relationship to privacy and security. For example, Rod noted that "it is very hard to protect your privacy with Facebook" and that he has "an apocalyptic sense of the future" where "it is this giant database of people."

4.3 There is no Privacy in the Brave New World

Like Patience (*Female, Age: 40 to 49*), whose words begin this paper, many of our participants believed that privacy is something in the past and no longer exists in the interconnected, technologically advanced world of today. Some noted how as soon as you connect (online implied) you have lost privacy, and many discussed how government, businesses, and the general public (including hackers) can (and do) access and store personal information, leading to a loss of privacy and a lack of security.

Doug explained (*Male, Age: 50 to 59*): "You put your name out there and it is already compounded, you can't stop it. Any information you put out there is no longer personal. There is no privacy, you are being watched everywhere." Geoff (*Male, Age: 50 to 59*) said: "The minute you let your guard down then your privacy is gone…but I don't think there's that much privacy in our society anyway. If people want to find things out they will." Mia explained (*Female, Age: 30 to 39*): "When the revolution comes – we are all going to be screwed because we are all in their databases." And Scot (*Male, Age: 60+)* said: "If you go on the network for any reason – privacy is almost eliminated. The network is open to the entire world."

Many of our participants still engaged in some behaviors to protect their privacy even after articulating how and why they thought privacy did not exist in the cyberworld. Patience (*Female, Age: 40 to 49*) delineated a host of precautions she takes to provide security and protect her privacy: strong passwords, signs of secure websites, and the use

of a firewall. She said: "It makes me totally paranoid when I see these shows where the guy is sitting there with an open router and picking up everything the person is doing. My cousin is sitting on an open network and I try to explain to him that 'dude it is like walking down the street totally naked'."

Actively engaging in practices to feel more secure and protect their privacy was true for many of those who questioned online privacy and security, representing just one of the ways in which participants had mixed experiences with, beliefs about, and behaviors toward online privacy and security.

Many of the participants who talked about the lack of privacy in the cyber world drew on a Fatalistic Model, noting that "If someone wants to get into my account they are going to get into my account" (*Lewis, Male, Age: 50 to 59*), or that "I guess I am resigned to data mining for marketing" (*Michelle, Female, Age: 40 to 49*). This sense of resignation was present in many of our interviews, and participants often noted how they had become immune to the worry about privacy and security. Viseau et al. found similar results where "participants' privacy perceptions seem to be associated with an attitude of resignation and even of total disregard for the whole subject of privacy" [3]. For example, Hank (*Male, Age: 20 to 29*) talked about "being desensitized to it, I know bad things can happen." Later, he talked about 'background noise' as he discussed security. For Hank, as for many other participants, it did not matter what they did, their privacy and security were going to be compromised in the online environment and it was out of their hands.

Often participants discussed this fatalistic view and then a bit later in the interview presented an Optimistic Model, where they described how everything was fine since nothing bad had happened to date. This cognitive bias of normalcy [19] grew out of a particular innocence about online environments and the potential consequences which Swanson et al., [2] call a "nothing to hide, nothing to fear" attitude.

Hank (*Male, Age: 20 to 29*) is one example. His previous comment about background noise was followed by: "I know that the risk exists and my security can be compromised and my information can be stolen. But I don't hear it happening often to my peers. I haven't heard horror stories of anyone getting my email." Similarly, Tiffany (*Female, Age: 20 to 29*) noted: "Because nothing has happened on my home computer I feel safe. I almost feel it is contingent on nothing happening."

Swanson et al., found similar results. They describe how their participants "trust that others would not victimize them, and believe that something bad is unlikely" [2]. They argue their participants were "naïve" and "guided by a false sense of security" something we also see in our data (p. 45).

It was not unusual for participants to present both a fatalistic and an optimistic perspective, demonstrating a lack of consistency in their understandings of and experiences with sharing and managing their information online. Both perspectives represent "a short-term vision of individual interests and preferences rather than a broader societal perspective" about online privacy and security (p.106) [3].

4.4 Online Privacy and Security: Multiple Mental Models

Participants often drew one mental model and in the next sentence articulating a different one as they describe their experiences with managing their information. Sometimes,

a participant utilized three or four different mental models over the course of an interview, often when describing the same thing. Occasionally these mental models would be used in the answer to just one interview question.

For example, at the end of his interview Hank (*Male, Age: 20 to 29*) was asked if he had any other thoughts or comments. He first answered by noting that no matter what he does it would not make much difference, and that if "it [something bad] is going to happen it is going to happen." He began by articulating the idea of not having control, of the online environment being in control. Two sentences later he presents a different idea, and within the space of a few minutes has laid out multiple mental models. "I have this perception that the Internet is less wild…there is less uncharted territory now. You can get confirmation from other people by going to forums that fifty thousand people use and go to trusted websites like Amazon, Google, and Facebook, and Twitter. I go to sites I have established relationships with and have reputations. I feel like unless you are looking for pirated software or going on foreign websites that they are more dangerous. And when I don't go to websites I know, I will do research when something sounds too generic or doesn't sound right. I am a borderline creepy 'Googler'."

Hank initially presented an image of the Internet as a wild place where no matter what he does that things can happen—he is not in control. But then he quickly goes on to describe the Internet as "less wild" with "less uncharted territory" than before. His words evoke the "Wild West" where there was often lawlessness and no control. However, now this wild world has been tamed; you know where to go and who you can trust with your information.

Hank drew on a Reputation Model as he talked about "trusted websites" that he has "established relationships with and have reputations." Like Hank, many of our participants generally limited online transactions to "vendors that we have had a relationship with" (*Mark, Male, Age: 50 to 59*). "I usually shop at places that I have heard of, reputable sites" (*Kendall, Female, Age: 20 to 29*), or "I just try to buy from certain places, like a brand, based on their reputation" (*Coco, Female, Age: 30 to 39*).

When participants used a Reputation Model it was to refer to specific places or brands that they already had developed a relationship with in the physical world. While Hank and other participants considered "reputation" as an indicator of safety, they did not (perhaps could not) describe how or why reputation provided greater security. This is another example of naïve users trusting sites, often based on "feeling" or "a sense" that they have.

Perhaps most interesting is that previously Hank talked about how taking security measures was useless since "it is out of my hands" using a Fatalistic Model to reinforce the lack of control. Yet in this final statement he notes that he is a "borderline creepy 'Googler'" who does research "when something sounds too generic or doesn't sound right" where he draws on a Verification Model when he needs to take action before he decides whether to share or withhold information.

Many participants demonstrated this back and forth in their thinking about online privacy and security. For example, Patience (*Female, Age: 40 to 49*) initially argued, "there is no privacy" today, but also said she is "very keenly aware of the problems that can come around." Later, she discussed how she has a firewall to protect herself, but later noted how "a lot of times I leave my credit card up there, I need to be a bit better

with my password, I just use a generic password" and that she gets very frustrated with sites that "give me too many blocks, then I'm going to be turned off." Participants seem to 'flip-flop' in their understanding of risk and their decisions about sharing, withholding, and managing their information online.

At another point in his interview, Hank specifically drew a distinction between at home versus at work security where security is not his responsibility and is relegated to someone else. "I assume my security at work is better because we have a whole group at work that does that. I feel safer at work and it is their job to protect that." Other participants said it was the responsibility of their bank or the website they used. We refer to this as a Not My Job Model, where participants believe the responsibility to provide security and protect privacy rests with someone else. Often, participants used this idea when speaking of banks. Rod (*Male, Age: 20 to 29*) explained: "The bank, it is their job, so they better be doing it." and John (*Male, Age: 50 to 59*) "I am looking for big time security. I rely on the banking sites to take care of that security." When participants relied on others to protect their privacy or provide security, they engaged in a form of "off-loading risk" and "transferring responsibility" to others and failed to see the ways in which such behavior might be risky [2].

Many participants, like John above (or Patience earlier), said they wanted "big time security" but did little or nothing to protect their security. In addition, participants, including Hank, drew on a model of Little Value, where they articulated how they did not think they had anything that others would want. Mia (*Female, Age: 30 to 39*) captures this model well in statements she makes. "I don't know why anyone would want any of my information. There is nothing in my background that anyone would want to steal. I am the most boring person on the planet and I have no money."

This model does not recognize the potential dangers out there or the reasons that others may want to access their information. Similarly in a study by Swanson et al., found that participants "operated under a perception that the things they might reveal would be of limited value to other parties" [2] or in the study by Viseau et al., where participants saw themselves as "simply not interesting enough to justify paranoia about privacy" (p. 105) [3].

Many of our participants used multiple mental models as they spoke of their experiences with sharing, withholding, and managing their information in the cyberworld. Like Hank, their models were often only partially formed, contradictory, and based on misinformation or faulty assumptions linked to real world rather than the online environments.

4.5 A Notable Exception: The 'Expert'

While we noted very few fully formed mental models that guided people's behavior as they talked about their experiences, there was one notable exception. Baldwin (*Male, Age: 30 to 39*) discussed online shopping and banking in the following way: "I have a fatalistic approach and I understand the system is fundamentally not perfect. I am not worried that someone is going to go through my trash and get my credit card number. It is much more likely that somebody will break into the credit card processor's computer and get a million accounts including mine. I still use a credit card even though it can be compromised and I consider it a necessary evil. So it is a tradeoff and the price that I pay for the convenience of having a bank account."

Baldwin realized there are tradeoffs and that the online system is flawed. He talked about the greater likelihood that his credit card will be stolen online. He acknowledged the ways the government and banks work to insure this does not happen. Later he actually used the words 'mental model' to explain how he deals with privacy and security as compared to his friends. "I have developed a mental model—when people buy a car they know they are not just going to pay for the car and it requires maintenance. I see a real lack of knowledge that people assume they buy a computer and it has Windows on it and that is all they have to do." Here, he drew on a Maintenance Model where you need to take care of your computer in order to insure security, just like you need to take care of your car.

5 Conclusions

Through their stories shared by participants in this study, we paint a picture of what privacy and security look like from their perspectives. This picture presents the landscape in what participants see as a brave new world, a world that is constantly shifting and changing, a world where "I am probably two weeks behind those who are out there to try and break into computers, forever two weeks behind" (*Edgar, Male, Age: 40 to 49*).

Mental models utilized by our participants include: Brave New World, Fatalistic, Little Value, Maintenance, Not My Job, Optimistic, Reputation, and Verification. Almost all participants drew on some notion of Brave New World, and of all the models we identified this seems to be the most common. But there was not one overarching mental model to guide them. Instead, they often drew on bits and pieces of multiple partially- or ill-formed mental models that represented their 'naïve' understandings of the cyberworld and its risks.

Viseau et al., argue that "individuals approach privacy from the context of their own actual practices, associating it with their individual experiences and concerns…" (p. 106) [3]. In order to develop successful online privacy and security educational initiatives, we must understand the varied and contextualized ways in which participants engage in collective information practices. "Talking about the need to maintain privacy and provide security, however, frames these concepts as stable and uniform features of the world, independent of the particular social and cultural circumstances in which individuals find themselves at particular moments" (p. 335) [1]. Online and computer privacy and security were not stable but rather fluid concepts, and dependent on the context and type of interaction. This assumption of an overarching and stable understanding of privacy and security may be why "at best, the privacy 'movement' is failing to meet its objectives, and that, at worst, it is misguided" (pp. 105-106) [3].

Many efforts to improve user understandings of cybersecurity focus on the moment when information is released into cyberspace, and not when users are sitting in front of the computer or interacting with it [3]. This may be one reason that users adopt a Fatalistic Model—one reason why they believe that whatever they do it will not matter and that their actions only impact them and not a broader community.

Education and training aimed at preparing better cyber-citizens in this brave new world must: (1) recognize the fragmented, fluid, and often naïve understandings of users; (2) draw on analogies that users currently hold; (3) focus on how we share, withhold,

and manage information and the social actions they are aimed at accomplishing; and (4) help users see privacy and security as more than just the moment when data is released. In addition, our data suggest that it is important to position online privacy and security as a communal issue, one that is larger than just the individual, in order to help users develop "more socially sound privacy practices" [3].

References

1. Dourish, P., Anderson, K.: Collective information practice: Exploring privacy and security as social and cultural phenomena. Hum.-Comput. Interact. **21**, 319–342 (2006)
2. Swanson, C., Urner, R., Lank, E.: Naïve security in a Wi-Fi world. Trust Manage. **4**, 32–47 (2010)
3. Viseau, A., Clement, A., Aspinall, J.: Situating privacy online: Complex perceptions and everyday practices. Inf. Commun. Soc. **7**, 92–114 (2004)
4. Wash, R.: Folk models of home computer security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security, p. 1–16. ACM, Redmond (2010)
5. Asgharpour, P., Liu, D., Camp, L.J.: Mental models of computer security risks. In: WOODSTOCK 1997, El Paso TX (1997)
6. Camp, L.J.: Mental models of privacy and security. SSRN (2006). http://ssrn.com/abstract=922735 or http://dx.doi.org/10.2139/ssrn.922735
7. Asgharpour, F., Liu, D., Camp, L.J.: Mental models of computer security risks. In: Work Shop on the Economics of Information Security (2007)
8. Sheehan, K.B.: Toward a typology of Internet users and online privacy concerns. Inf. Soc. **18**(1), 21–32 (2002)
9. Brandeis, L., Warren, S.: The right to privacy. Harvard Law Rev. **4**, 193 (1890)
10. Schoeman, F.: Philosophical Dimensions of Privacy. Cambridge Press, Cambridge (1984)
11. Hoffman, L.: Computers and Privacy in the Next Decade. Academic Press, New York (1980)
12. Furman, S., Theofanos, M.F., Choong, Y.Y., Stanton, B.: Basing cybersecurity training on user perceptions. IEEE Secur. Priv. **10**(2), 40–49 (2012)
13. Charmaz, K.: Constructing grounded theory: a practical guide through quantitative analysis. SAGE, Thousand Oaks (2006)
14. National Research Council: Toward better usability, security, and privacy of information technology. National Academies Press, Washington DC (2010)
15. Dourish, P., Grinter, R.E., de la Flor, J.D., Joseph, M.: Security in the wild: userstrategies for managing security as an everyday, practical problem. Pers. Ubiquit. Comput. **8**(6), 391–401 (2004)
16. Hruschka, D.J., Schwartz, D., John, D.C.S., Picone-Decaro, E., Jenkins, R.A., Carey, J.W.: Reliability in coding open-ended data: Lessons learned from HIV behavioral behavioral research. Field Methods **16**, 307–331 (2004)
17. Stokes, J.: Understanding Moore's Law. ars technica. Accessed on 09 Sep 2014, 27 Sep 2008
18. Schaller, B.: The Origin, Nature, and Implications of "Moore's Law". Research Microsoft. com. Accessed on 22 Aug 2011, (26 Sep 1996)
19. Hutton, D.: Lessons unlearnt: the (human) nature of disaster management, emergency management. In: Eksioglu, B. (ed.) Operations Management. InTech, Rijeka (2012). ISBN: 978-95307-989-9, doi:10.5772/35019. http://www.books/emergency-management/lessons-unlearnt-the-human-nature-of-disaster-management