Challenges in Supporting End-User Privacy and Security Management with Social Navigation

Jeremy Goecks, W. Keith Edwards, and Elizabeth D. Mynatt
GVU Center, College of Computing
Georgia Institute of Technology
Atlanta, GA 30332
{jeremy, keith, mynatt@cc.gatech.edu}

ABSTRACT
Social navigation is a promising approach for supporting privacy and security management. By aggregating and presenting the choices made by others, social navigation systems can provide users with easily understandable guidance on security and privacy decisions, rather than requiring that they understand low-level technical details in order to make informed decisions. We have developed two prototype systems to explore how social navigation can help users manage their privacy and security. The Acumen system employs social navigation to address a common privacy activity, managing Internet cookies, and the Bonfire system uses social navigation to help users manage their personal firewall. Our experiences with Acumen and Bonfire suggest that, despite the promise of social navigation, there are significant challenges in applying these techniques to the domains of end-user privacy and security management. Due to features of these domains, individuals may misuse community data when making decisions, leading to incorrect individual decisions, inaccurate community data, and "herding" behavior that is an example of what economists term an *informational cascade*. By understanding this phenomenon in these terms, we develop and present two general approaches for mitigating herding in social navigation systems that support end-user security and privacy management, mitigation via algorithms and mitigation via user interaction. Mitigation via user interaction is a novel and promising approach to mitigating cascades in social navigation systems.

Categories and Subject Descriptors
H5.3 [**Information interfaces and presentation (e.g., HCI)**]: Group and Organizational Interfaces - *collaborative computing, theory and models*. K4.1 [**Computers and Society**]: Public Policy Issues – *privacy*.

General Terms
Design, Human Factors.

Keywords
Acumen, Bonfire, social navigation, herding, informational cascades, end-user privacy and security, decision making.

1. INTRODUCTION
A social navigation system is a collaborative computing system that collects and aggregates behaviors, decisions, or opinions from a user community and displays this information to individuals to guide their behavior or inform their decision making [14]. There has been substantial research in social navigation systems [27], and researchers have applied social navigation systems to many diverse domains [26, 36, 44, 48, 53].

Social navigation systems, however, are not just of academic interest; social navigation systems are an integral component of numerous businesses, pointing users toward highly rated posts on discussion forums, frequently downloaded recipes in an online cookbook, and recommendations for songs that a user may be interested in purchasing from an online store. Many highly popular websites use social navigation systems either as a primary or complementary component of their site, including the online store Amazon, the technology news and discussion website Slashdot, and the websites for the news organizations BBC and *The New York Times*.

Social navigation is a promising approach for supporting end-user privacy and security management. Since many users are unmotivated to manage their privacy and security [16, 54] and do not understand the technical issues associated with privacy and security management [22, 46], social navigation systems can provide a new, simpler approach to informed decision making. For example, since prior research has shown that users often prefer to delegate privacy and security management to others [16], social navigation can provide for such delegation: a user that is unsure about how to manage his privacy or security can simply choose to follow the community's majority decision.

We have developed two prototype systems to explore how social navigation can help users manage their privacy and security. The Acumen system employs social navigation for privacy management; Acumen helps individuals manage their Internet cookies both manually and automatically based on the behavior of others [20]. The Bonfire system uses social navigation for security management; Bonfire is a personal firewall that uses multiple types of social navigation data to help users make firewall management decisions.

Our experiences with Acumen and Bonfire suggest that, despite the promise of social navigation in security and privacy applications, there are significant challenges in applying the technique in these domains. In particular, due to the types of decisions and general lack of expertise among users in these domains, individuals may make incorrect inferences from a social navigation system's community data and misuse community data when making decisions. These incorrect inferences and misuse of community data can lead to incorrect individual decisions,

Symposium On Usable Privacy and Security (SOUPS) 2009, July 15-17, 2009, Mountain View, CA, USA.

inaccurate community data, and "herding" behavior in which a community consensus builds for an incorrect decision.

These challenges serve as the motivation for this paper. We argue that these challenges are due to *informational cascades* that can arise in these systems. Informational cascades are an economic concept and the subject of considerable research; cascades occur when individuals, faced with a decision, ignore their own information and choose to go with the majority decision, thereby creating a herd or cascade [4, 6, 52]. An analysis of Acumen and Bonfire indicates that mitigating informational cascades is necessary if social navigation systems are to be useful for privacy and security management.

We discuss two general approaches for mitigating cascades in social navigation systems, mitigation via algorithms and mitigation via user interaction. Given the weaknesses of using an algorithmic approach to mitigating cascades, we propose that employing user interaction techniques is a promising approach for mitigating cascades. Both approaches have merit but require tradeoffs and are dependent on features of the sociotechnical system surrounding the privacy or security management activity and its supporting social navigation system.

We offer three contributions in this paper. First, we describe two systems that apply social navigation to support common privacy and security management activities, as well as our experiences with these systems and the challenges of using social navigation in these contexts. Second, we analyze these challenges in the context of informational cascades research and argue that mitigating cascades can improve the utility of social navigation systems for privacy and security management. Third, we describe two general approaches for mitigating cascades in social navigation systems targeted at end-user privacy and security management: mitigation through algorithmic strategies and mitigation through user interaction techniques.

2. ADDRESSING END-USER PRIVACY AND SECURITY MANAGEMENT WITH SOCIAL NAVIGATION

It is important to establish why social navigation might be useful for supporting end-user privacy and security management; this understanding provides the foundation for analyzing the efficacy of social navigation systems applied to privacy and security management. We define "end-users" to mean users that have no special or explicit training in managing their privacy or security.

There are similarities in how users think about privacy management and security management. Previous research argues that people perceive privacy management to be a boundary management process, and potential privacy boundaries include temporal, interpersonal, and boundaries between a private and public sphere [39]. Similarly, there is evidence that users perceive security as a barrier which should "keep things out," regardless of whether those things are privacy threats or security threats, and that controlling and configuring this barrier is a key activity in security management [16].

In general, when a user manages a boundary for the purposes of meeting privacy or security needs, she is making decisions about where to place the boundary, what can cross the boundary, and when to change the boundary to meet current context and constraints. While this is a very general description of boundary management, there is one commonality among most boundary management activities: decision making—both implicit and explicit—is the core activity of boundary management. It is unreasonable to attempt to automate all privacy and security management decisions due to numerous technical and social factors that limit the efficacy and acceptance of such automation [17]. Thus it is important to explore solutions that help users make good decisions when managing their privacy and security.

In this paper, then, we focus on the decision-making processes that users engage in when performing the boundary management activities associated with meeting their privacy or security needs. Thus, our references to privacy and security management refer to the decisions that users must make to create, adjust, and update their privacy and security settings. Furthermore, we focus on the challenges that users face when making these decisions and how social navigation can address these challenges.

There are two common issues that end-users face when making privacy and security management decisions. First, end users often do not understand the technical issues associated with privacy and security management and, lacking this understanding, users cannot make informed decisions [46]. For instance, when managing a personal firewall, users often must understand what a process is, what a port is, and what it means to block a process or port from accessing the Internet. In addition, abstractions, such as access policies, are common in computer security but problematic for end users [54], and privacy management is frequently confounded by complex settings (e.g. [37]).

Another barrier for effective end-user privacy and security management is motivation. Most users are uninterested in the technical details of computer security [22] and lack the incentives and time to effectively manage their security [16]. A main reason for users' low motivation is that security is frequently a complementary task, performed alongside or in conjunction with a primary task [54].

Low motivation to engage in privacy and security management activities leads users to engage in particular behaviors. First, users often seek to spend as little time as possible on security and thus make security decisions quickly, do not experiment with security settings, and do not revisit past security decisions [25]. Second, many users try to delegate privacy and security management to other people [16]. In many instances, however, users may struggle to find delegates because expertise in privacy and security management is rare.

2.1 Matching Social Navigation to End-user Security and Privacy Management

Social navigation has the potential to address the common problems in end-user privacy and security, and hence we posit that social navigation is a promising approach for helping users make decisions when managing their privacy and security.

Social navigation systems enable a user to see what other people have been doing or saying by automatically capturing, aggregating, and displaying the behavior and activities of its community of users [14]. For example, a social navigation system might provide "paths" based on previous user behavior that lead to the most highly rated posts in a discussion forum, the most frequently downloaded food recipes from an online cookbook, recommendations for songs that a user might be interested in purchasing from a music store, or—in the case of Dourish and

Chalmers' original work—navigation of information spaces based on social activity rather than spatial markers [14].

Researchers have built systems that enable users to navigate socially in numerous domains; some of these domains include editing and reading documents [26], reading newsgroup messages [44], exploring an online food recipes store [48], browsing the Internet [53], finding citations for research papers [36]. Many highly popular websites use social navigation systems either as a primary or complementary component of their site, including the online store Amazon, the technology news and discussion website Slashdot, and the websites for the news organizations CNN, BBC, and *The New York Times*.

Recall that one challenge users face when making decisions to manage their privacy or security is understanding the technical issues associated with a decision. Using social navigation systems to support privacy and security management means that users have an additional source of data in the system's community data, and this data may be easier to understand and use than the technical data typically associated with privacy and security decisions [25]. Also, people often are able to learn quickly by observing others [3], and social navigation supports this type of learning as well.

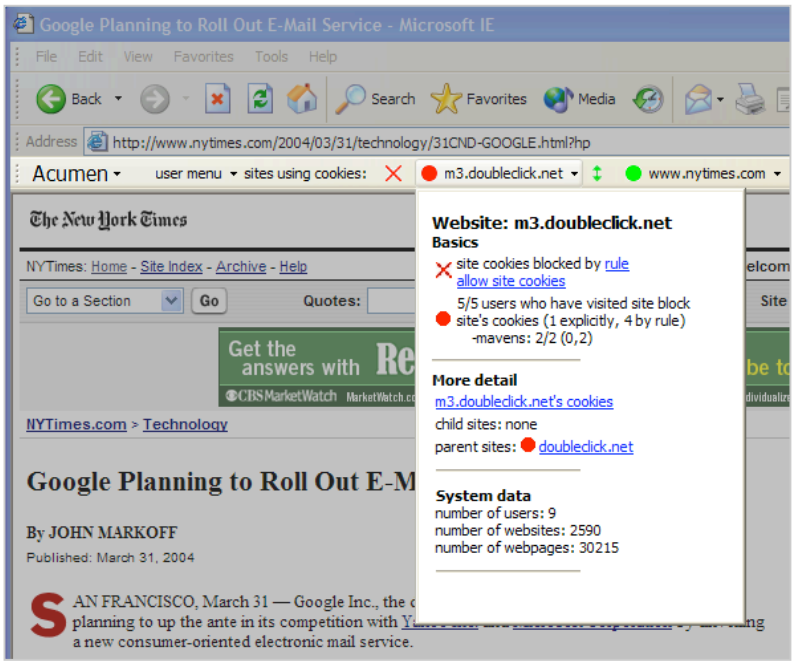

Figure 1. Acumen toolbar for a page on *The New York Times* website.

The other principal challenge in privacy and security management is low motivation among users and their preference for delegating privacy and security management [16]; social navigation can address this challenge as well. A simple social navigation system that collects and displays a community's actions and decisions imposes minimal burden on users, and thus individuals can participate and use a social navigation system with nominal effort. Social navigation systems provides a way for users to delegate their decisions to others: a user that is unsure of how to manage his privacy or security can simply choose to follow the community's majority decision.

Finally, preliminary research has analyzed how social navigation might be applied to end-user privacy and security management. An analysis of user help techniques for end-user security applications suggests that social navigation is amongst the most natural and straightforward forms of help and learning, though it does requires interpretation of community data [25]. DiGioia and Dourish recently discussed how social navigation might help users understand patterns of conventional use and the activities of others [12]. Our research builds on this work, taking significant steps to understand how social navigation helps users make decisions to manage their privacy or security and what challenges arise from using social navigation in these domains.

3. SUPPORTING END-USER PRIVACY WITH SOCIAL NAVIGATION

This section describes our experiences applying social navigation to help users manage a common Internet privacy problem.

3.1 The Problem: Managing Web-browser Cookies

A common privacy concern that Internet users have is the collection of personal data by third parties; users want the ability to control when, how, and what information they share with third parties [32, 38]. Internet cookies are particularly troublesome in this respect because websites can use cookies to collect and store information about users; sites often use cookies to monitor users' browsing activities. In fact, at least thirty-five percent of websites use cookies to collect such information [18].

Much work has been done to help users manage their cookies. Many online privacy policies describe how a website uses cookies and what data they collect using them, but online privacy policies are often difficult to locate and understand [31]. The Platform for Privacy Preferences (P3P) specification enables websites to encode a privacy policy in a machine-readable format; software agents can then interpret and utilize P3P policies [8].

Both of today's major browsers, Internet Explorer and Firefox, provide users with the ability to manage cookies in various ways. However, studies of past versions of these browsers show that there are problems and inadequacies with both browsers' cookie management tools, such as making them hard to find and modify, providing little on-going awareness of cookies, and using terminology that users do not understand [19, 37]. Recent studies show that while awareness of cookies is growing, many users are not knowledgeable enough to manage cookies effectively [30, 41].

3.2 Acumen

We developed the Acumen system [20] (Figure 1) to help users manage their web-browser cookies. We used an iterative design process to develop Acumen, ultimately completing six full iterations. During each iteration, we developed numerous interface prototypes, presented the most promising prototypes to a mix of HCI practitioners, privacy experts, and everyday users, and obtained feedback from them. We obtained feedback from a mix of individuals in order to gather data from individuals with different levels of expertise and diverse perspectives. Practitioners and experts were quite important to the process because they provided insights that users did not, especially the potential

problems that users might have in using Acumen's community data. We employed the feedback obtained during each iteration to refine and select techniques from both social navigation systems research and digital privacy management research for subsequent iterations.

Acumen integrates with a browser's standard cookie management functionality; users manage cookies at the website level, allowing or blocking cookies from websites. Acumen allows all cookies by default. As a user browses the web, Acumen provides information about the websites that are using cookies on the pages that he visits and community data for these websites. When a users visits a webpage, Acumen displays the websites using cookies on the page and next to each website, an icon that summarizes the community data for the website.

Acumen's community data consists of the number of users who have "visited" a website (i.e. requested a file from the site), the number of such users who allow the site's cookies, and the number of users who block the site's cookies. Collecting and displaying this simple form of community data has proven successful for promoting awareness and supporting decision making in the past [26, 48, 53]. Acumen encodes its community data in a circle icon using colors established by the Privacy Bird application [8]; using a colored icon as the primary indicator has been shown to be effective in providing information to users when they are making a privacy decision [9].

Users can leverage Acumen's community data in multiple ways. Like the Privacy Bird, Acumen enables a user to maintain awareness of ongoing privacy actions and changes via a persistent, peripheral interface near the top of the web browser. Acumen's interface enables a user to maintain awareness of (a) the websites using cookies on the web pages that she is visiting and (b) whether other community members generally allow or block cookies from these sites. When making the decision to allow or block a website's cookies, users can view the site's community data in detail and use this information to inform their decision.

Users can also employ simple rules that leverage community data to automatically block cookies. Users can create rules of the form 'If X% of users have blocked cookies from a website, then automatically block the site's cookies.' Users choose a rule's threshold percentage when they create it. To the best of our knowledge, using community data to automate actions is novel; we implemented this feature in an effort to help users more easily delegate cookie management to the community.

A concern that became prominent when we were designing Acumen is herd behavior [4]. In herd behavior, individuals unsure of a decision often choose to follow the majority—the herd—causing the herd to grow, which then leads even more individuals to follow the herd. Herding behavior can continue via this cycle for a long time, and if users build a consensus for an incorrect decision, many users can be misled and thus choose the incorrect decision.

Herd behavior is especially likely in Acumen for two reasons. First, most users have little knowledge of cookie management and thus are likely to follow the majority decision. Secondly, herd behavior is likely because users cannot delay making management decisions about cookies, even if there is very little community data to help them. When a user visits a webpage using cookies, he must choose whether to allow or block those cookies immediately, even if there is limited community data. Decisions made with less community data are often more prone to herding behavior because there is less information contained in the data [4].

We discuss herding in much detail later in the paper, but for now it suffices to note that herding in social navigation systems has not been well addressed.

In an effort to mitigate bad herding behavior—herding behavior that leads to poor, incorrect, or uninformed decisions—Acumen provides community data from a select subset of 'experts.' Acumen leverages experts' knowledge by anonymously identifying and providing community data from them. We posited that providing expert community data would help mitigate bad herding behavior and also promote good herding behavior, in which uninformed users followed experts.

To identify experts, Acumen computes an 'expert rating' for each individual, based on a user's breadth and depth of cookie management activity. Acumen labels users with the top 20% of ratings as experts and encodes the experts' community data as a smaller circular icon embedded in the large community data icon. Embedding the experts' data this way makes it easy for users to see the expert data and contrast it with the overall community data.

3.3 Lessons Learned from Acumen

We conducted a limited, controlled deployment of Acumen, making it available to nine users for six weeks so that we could better understand the questions we encountered during its design. At the end of the six weeks, Acumen's database contained data for over 2650 websites; users had blocked cookies from 85 websites using Acumen. We learned two lessons from our design and deployment of Acumen.

Firstly, Acumen helped users make good decisions for cookies with clear decision criteria. To evaluate users' decisions, we employed results from multiple Internet privacy studies [1, 18, 23, 50] to develop a model for labeling cookies (Figure 2). Two dimensions comprise this model: (1) the amount of trust in a cookie's website and (2) the benefit-cost ratio of using a cookie. Using this model, we applied one of four labels to each website's cookies: (a) good; (b) bad; (c) future investment; or (d) high risk, high reward.

Acumen's users generally allowed *good* cookies—which had a high benefit-cost ratio and high trust—and blocked *bad* cookies—which had a low benefit-cost ratio and low trust. However, for cookies labeled as *future investment* or *high risk, high reward*—which have a more complex or ambiguous relationship between benefit-cost ratio and trust—Acumen proved less useful as users disagreed about whether to allow or block such cookies.

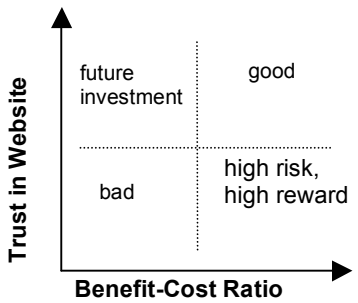

Figure 2. Cookie label model.

Another way to state this finding is that Acumen's community data proved useful for making objective decisions—decisions where personal preferences or biases were relatively unimportant in the decision-making process—and less useful for subjective decisions.

Secondly, in interviews, six of nine users indicated that they engaged in herding behavior and blocked a site's cookies based solely or largely on community data. It was difficult to determine whether experts' community data was useful in mitigating herd behavior due to the small number of users in our deployment. That said, three of nine users indicated that they were skeptical that experts were more knowledgeable than other users and chose to use community data from all users rather than experts' data.

4. SUPPORTING END-USER SECURITY WITH SOCIAL NAVIGATION

This section describes how social navigation can be applied to address a classic end-user security management problem: personal firewall management.

4.1 Personal Firewall Management

A personal firewall is software that enables an individual to control the data flow between his computer and the Internet; typically, a user controls this data flow by granting or denying software applications on his computer access to the Internet. Personal firewalls are increasingly important because pervasive, persistent, and high-bandwidth connections to the Internet are becoming common both in the home and in public (via wireless hotspots) [28, 40]. More than half of all broadband users have installed a personal firewall [42].

Persistent, high-bandwidth connections to the Internet pose numerous security and privacy risks to users. These connections make it easy for users to download, run, and accidentally share malicious software—such as software that attempts to obtain passwords or financial records for use in identity theft.

Data flow between a user's computer and the Internet also has privacy implications. For instance, there are applications that report information about an individual's activities back to web servers on the Internet, such as his web browsing activities[1] and whether he read an email message[2]. Finally, general annoyances also arise from data flow issues; popup windows from spyware often occur because the spyware is connecting to another computer on the Internet.

End users can significantly alleviate these problems by using a personal firewall effectively; effective use of firewalls means making good decisions about which programs are allowed to connect to and send and receive data from the Internet.

Unfortunately, using a personal firewall effectively is difficult because personal firewalls suffer from two significant end-user security management problems discussed earlier: (1) firewall management is a complementary activity to other primary activities, such as sending and receiving email, browsing the Internet, and updating software; and (2) firewall management often requires users to understand technical information—such as IP addresses, ports, and processes—in order to complete primary tasks [24].

[1] http://www.zango.com
[2] http://www.didtheyreadit.com

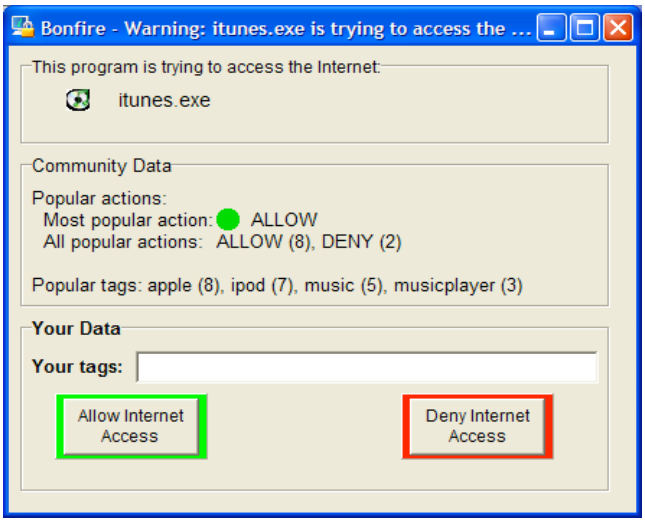

Figure 3. Bonfire alert window.

4.2 Bonfire

Bonfire (Figures 3 and 4) is a personal firewall infused with a social navigation system. With Bonfire, in addition to exploring the application of social navigation to a new problem domain, we also wished to focus on mitigating herding behavior based on lessons learned from Acumen.

We again used iterative prototyping to design Bonfire. We repeatedly developed prototypes of Bonfire's interfaces, presented them to HCI practitioners, security experts, and everyday users to get feedback, and applied their feedback to refine and select techniques from the social navigation and security management bodies of research. We performed a total of seven iterations to create Bonfire.

Bonfire provides functionality comparable to other popular personal firewalls, notifying a user via a popup alert window (Figure 3) when a firewall management decision must be made. Bonfire notifies a user when a program on his computer attempts to access the Internet or tries to receive connections from Internet. Bonfire also provides a summary window (Figure 4) where users can view current rules, create new rules, and delete unwanted rules. Rules dictate the programs that can access the Internet and those that cannot.

Bonfire's community data is organized around programs (e.g. itunes.exe, mysearchbar.exe); for a program, Bonfire records the number of users who have allowed a program Internet access and the number of users who have blocked the program's access. Bonfire uses this community data in multiple ways throughout its interfaces. Bonfire also enables users to employ tagging [15, 47] as a supplementary community data source in Bonfire. Tagging is the practice of applying multiple, short words or phrases to describe an item; each word or phrase is an independent tag that describes the item.

Bonfire presents community data in a section of its alert window. At the top of this section is the most popular action that the community has taken when faced with this decision. This information is presented as text and via a colored circle that corresponds to the background color of the decision buttons at the bottom of the window. The purpose of this correspondence is to reinforce the connection between Bonfire's community data and

the user's decision. Using a colored icon as the primary indicator, as Bonfire does for its community data, has been shown to be effective in providing information to users when they are making a security decision [9].

Next, more details of Bonfire's community data are provided in the form of 'popular actions.' This is a list of frequent decisions that the community has made, and this information includes, in parentheses, the number of users that have made each decision. For some firewall decisions, there are more than two choices, hence our use of 'popular actions,' which can accommodate multiple options.

Finally, Bonfire shows the most popular tags that users have applied to the program. Tagging is a response to the herding behavior that occurred in Acumen and is likely to occur in Bonfire for the same reasons. Many users lack sufficient technical knowledge to use firewalls [24] and hence were likely follow the majority decision. In addition, there were likely to be instances in which users were faced with a firewall management decision and for which there was little community data, and herding towards incorrect decisions is more likely with relatively little data [4].

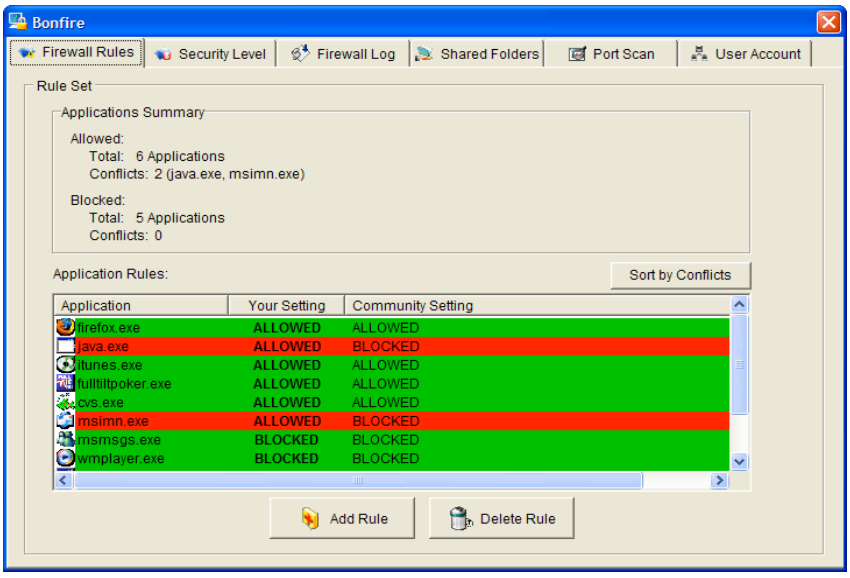

Figure 4. Bonfire's summary interface for viewing firewall rules.

Because we found that promoting good herding behavior in Acumen was quite challenging, we focused on mitigating all herding in Bonfire. Feedback on early iterations of Bonfire suggested that herding might be mitigated by providing additional information to supplement Bonfire's existing community data, such as why others blocked a program's Internet access or the context in which decisions were made.

For these reasons, we chose to use tagging as an additional source of community data. Tagging occupies a "sweet spot" among community data types for a social navigation system. Tagging imposes a low burden on users, yet tags are relatively easy to understand and use. Tags are often used to facilitate searching and navigating, but we expect them to play a different role in Bonfire. We anticipate that Bonfire's users will apply tags to a program to describe it or indicate why they blocked it. Bonfire's community data types are intended to complement each other. Bonfire's decision data summarizes the community's actions, and the tagging data provides information about why those actions were taken.

In Bonfire's alert window, tags that users have applied to a program are below the popular actions. As with popular actions, the number in parentheses next to a tag is the number of people who have applied the tag. Lastly, the alert window provides a section for a user to input her own tags for the program and make a decision for this firewall management question.

Bonfire's summary window (Figure 4) provides an overview of the application rules that a user has created and color-codes the rules to indicate whether the user's decisions agrees (green) or disagrees (red) with Bonfire's community data. This interface makes it easy for users to quickly identify which of their decisions differ from the community norm and revisit those decisions as needed.

4.3 Lessons Learned from Bonfire

We have learned much from our experiences with Bonfire. Unlike web-browser cookie management, personal firewall management is comprised mostly of *objective* decisions. That is, when users manage their firewalls, they are likely to manage them in similar ways; most users employ their firewall to block spyware, adware, and other malware, and users generally agree on what constitutes malware.

While there are individual differences in firewall management (e.g. some users will open particular ports to play online multiplayer games), the majority of decisions that users encounter are objective. This is in contrast to the privacy domain targeted by Acumen, in which there are a variety of decision types—subjective decisions, rooted in users' own orientation toward privacy and their daily routines of site visitation, and objective decisions guided by the identification of certain sites as misusing cookies or posing a true risk to users' privacy. We discuss objective and subjective decisions and their relationship to social navigation in section 5.1

In Bonfire, we identified a promising approach to mitigating herding behavior by combining activity-based community data—data about what other people are doing—and tagging. This approach provides insight into why herding behavior may occur: users may have difficulty interpreting and using solely activity-based community data to make privacy and security management decisions. Tagging provides a more explicit form of community data that complements the decision-based community data by providing information about why users made decisions.

5. REFLECTIONS: UNDERSTANDING HERDING IN PRIVACY & SECURITY MANAGEMENT

Our experiences with Acumen and Bonfire suggest that the user experience of social navigation in end-user security and privacy management is *qualitatively different* than that of other domains. These differences lead to herding behaviors that are not typically

seen in other social navigation systems, and yet are especially damaging in the security and privacy contexts.

In this section we explore the unique challenges that are inherent in the security and privacy domains themselves; these challenges are rooted in the distinction we make between subjective and objective domains. We also step back to make a connection between the herding behavior seen in these domains and the theory of information cascades, which can serve as a lens through which to better understand social navigation and shed light on opportunities to mitigate herding.

Concisely, our argument in this section is that when a user encounters an objective decision—as is the predominant decision-type in privacy and security management—he attempts to infer information from a social navigation system's community data and uses the inferred information to make a decision. If not accounted for in a social navigation system's design, use of a system's community data as an inferential information source can lead to herding behavior and render the community data uninformative or even incorrect. Uninformative or incorrect community data then leads to numerous and potentially a great number of incorrect decisions.

5.1 Subjective vs. Objective Decisions

Traditionally, social navigation systems have been applied to domains such as music, movies, recipes, and books. In these domains, the system's goal is to help a user make decisions that lead to items that appeal to her; in other words, the perspective that matters in these domains is that of individual users. These domains are described as *taste-based* or *subjective domains* because the evaluation criterion is subjective.

In contrast, *objective domains* are domains where users share evaluation criteria and thus agree on a desirable answer or goal state. Oftentimes, however, the desirable answer or state is not known in advance. We are not aware of any social navigation systems that have been applied to largely objective domains, with the exception of the Acumen and Bonfire systems described here.

For instance, many firewall questions fall into an objective domain. Users agree that they do not want malware to connect to the Internet because the malware can do damage to their computers. All users, then, will choose to block a software program from accessing the Internet if it is known to be malware. In summary, users agree on an evaluation criterion—is the software malware?—and the desirable decision, blocking malware from accessing the Internet. The challenge for a social navigation system applied to firewall management, then, is helping users decide whether to block a new program that may be malware.

Very few domains are completely subjective or objective, but most domains have more objective decisions or more subjective decisions. For example, one might posit that domains with a strongly objective flavor might include finances (in which maximizing wealth is an objectively "better" decision), healthcare, and the privacy and security domains described in this paper.

An important difference between subjective and objective domains concerns how well users are able to make sense of the community data that a social navigation system provides.

In subjective domains, an individual can often readily understand the basis of community data and thus make inferences from the data. Community data in a subjective domain arises from user preferences. An individual viewing community data can be confident that (a) users know their personal preferences and (b) users are making decisions that reflect those preferences, such as buying a book or choosing a recipe because they appeal to their interests. An individual viewing community data, then, can infer that users are making decisions with ample knowledge and acting according to that knowledge. These inferences are intuitive and allow an individual to use community data as an authentic information source when making decisions in subjective domains.

However, this logic frequently does not hold in privacy and security management. Managing one's privacy and security can be complex, and users often have limited expertise in these domains. Unlike subjective domains, where it can be assumed that users know their personal preferences and act on them, it is problematic to assume that others have expertise in objective domains and that they are acting on their expertise because this assumption may be incorrect.

When using community data to make privacy and security management decisions, then, this lack of knowledge about others' expertise makes it difficult for an individual to accurately infer information from community data and use the data as an authentic information source. This is a key difficultly in using social navigation to support decision-making in privacy and security management.

5.2 Informational Cascades

Our experiences with Acumen and Bonfire indicate that many users welcome community data from a social navigation system to help them make privacy and security management decisions because they are often unsure of their own decisions. When users are unsure of their decision, they are very apt to go along with the community consensus, which is made visible through a social navigation system's community data.

Of particular note is that users often go along with the community consensus even when they have information that suggests a decision different than the consensus. If enough users engage in decision-making this way, the result is herding within a social navigation system, and this herding is sustained and even amplified by the system's presentation of community data. Economists call this type of herding an *informational cascade* [4, 6, 52].[3]

In informational cascades, users who are unsure of their own expertise look to community data for guidance. Naturally, uncertain users often choose to follow the community consensus, and their decision is added to the system's community data. However, subsequent users viewing the community data assume the data derives from users with expertise rather than users who are uncertain. If enough users misinterpret community data this way, an informational cascade forms. Informational cascades lead to a false majority within a social navigation system, and the system's community data does not accurately reflect the

[3] Herding can arise from either normative influence, a tendency to use others' behavior as a means to conform to the social norm, or from informational influence, a tendency to use others' behavior as a source of information [10]. In our studies of Acumen and Bonfire, we found the most likely explanation of herding in these systems is informational influence. Hence, the herding in Acumen and Bonfire are informational cascades.

community's knowledge. Cascades, of course, can persist for some time and can lead users to many suboptimal decisions.

Understanding herding through the lens of information cascades not only sheds light on the underlying causes of herding, but—as we explore in the next section—provides a grounding for opportunities to mitigating herding through algorithmic and user interaction approaches.

In order to address informational cascades in social navigation systems applied to privacy and security management, it is useful to briefly survey previous research in cascades and social navigation systems. Informational cascades are a general socioeconomic phenomenon and are paradoxically named: they arise not from a plethora of information but *from a lack of information*. Informational cascades occur when individuals, acting in sequence and having observed the decisions of those before them, ignore their own information and make the same decision as the majority of others have previously made. Following the majority decision is rational from individual decision makers' perspectives, but the group cascade behavior is irrational.

Economists have studied the theory of informational cascades [4, 6, 52] and the frequent, real-world occurrences of informational cascades in numerous domains, including financial markets [11, 51], nutritional recommendations [49], fashions [6], information technology adoption [51], and website popularity [29]. Cascades occur at a surprisingly high rate. Theoretically, cascades occur at a rate of at least 12% if individuals' private information is 66% accurate [6]. In experiments, cascades occurred about 80% of the time that they are theoretically possible [2]. Moreover, individuals are often unable to recognize cascade behavior in others and thus unable to avoid participating in cascades [21][4].

Cascades do not necessarily lead to bad decisions. However, because it is not possible to predict in advance whether a cascade will lead to good or bad decisions, it is often better to mitigate cascades because a cascade that leads to bad decisions can have significant negative consequences due to the speed and size with which cascades can propagate bad decisions.

There are three necessary conditions for cascades to potentially occur:

1. sequential decision-making among a series of users;
2. individuals can see what decisions others have made;
3. discrete set of choices.

The first two criteria afford the opportunity for earlier decisions to influence later decisions, and the last criterion makes it difficult for an individual to make a decision that reflects both his private information and the information he infers from others' decisions.

Social navigation systems meet these three criteria for informational cascades. Social navigation systems afford sequential decision-making by aggregating community data and thus ensuring it is available to subsequent users. By definition, social navigation systems enable users to see what decisions others have previously made. Finally, social navigation systems nearly always offer a discrete set of choices, such as a set of hyperlinks to choose from or, in the case of privacy and security management, a set of choices for a particular decision.

Given that social navigation systems meet the informational cascades criteria, it is unsurprising that there is evidence of cascades in social navigation systems other than Acumen and Bonfire. In an online food and recipe store that supported social navigation, researchers reported that it was necessary "to watch out for the snowball effect where the social trails lead more and more users down a path they do not perceive valuable in the long run." [48] Online discussions forums that employ moderation to change message visibility for readers show evidence that informational cascades occur both to increase and to decrease message visibility [33]. Recommender systems researchers have also found evidence of cascade behavior: if users are asked to (re)rank a movie and are also shown the community's rating, their rank tends toward the community rating [7].

6. MITIGATING CASCADES IN SOCIAL NAVIGATION SYSTEMS

Informational cascades are an especially prominent problem for social navigation systems applied to end-user privacy and security management. There is ample evidence that users have little expertise in managing their privacy and security and struggle to acquire expertise. Users, then, are quite uncertain about their ability to make effective management decisions, and informational cascades research shows that higher uncertainty leads to a higher incidence of cascades.

Cascades cannot be mitigated simply by using more complex social navigation systems. Acumen and Bonfire use a very simple aggregation algorithm, counting the number of users that have made a particular decision and presenting this data to users. More complex social navigation systems use collaborative filtering to present users with personalized recommendations [44]. However, all types of social navigation systems present community data to users about how others behaved or what others decided. By presenting community data, irrespective of what algorithm was used to aggregate it, a social navigation system becomes susceptible to cascades. Recall that the previous section described how cascade behavior has been observed in both simple social navigation systems and in more complex, collaborative filtering systems.

However, by understanding the features of social navigation systems that lead to information cascades, we can begin to open up new opportunities for mitigating the cascade behavior that is so problematic in the security and privacy management domains. By mitigating these cascades, we can help ensure that the community data from the system is an accurate reflection of the community's knowledge and represents a "best guess" for a given privacy or security management decision.

In this section, we discuss two methods for potentially mitigating cascades: via algorithmic strategies and via user interaction techniques. Given the challenges associated with using algorithmic strategies to mitigate herding, we argue for a novel approach to mitigation that employs user interaction. We also anticipate that these approaches may prove complementary.

[4] The number of individuals that must engage in cascade behavior—following the community consensus rather than private information—in order for a sequence of decisions to be labeled as a cascade can vary. In general, at least 25% of individuals must consecutively engage in cascade behavior in order for a decision sequence to be labeled a cascade.

6.1 Mitigation via Algorithms

Recent research demonstrates that algorithmic approaches can yield a manipulation-resistant recommender system by limiting the influence of users whose ratings have proven to be inaccurate and thus potentially malicious; hence, users whose ratings have proven to be inaccurate in the past are limited in their ability to influence future ratings [45]. Similarly, there is algorithmic research on networks that has studied where to place detectors to identify cascades in the network [34] and how best to start cascades [13].

While these approaches provide a foundation for approaching cascade mitigation via algorithms, it is unclear how applicable they are to mitigating cascades in social navigation systems. Many informational cascades are started inadvertently and not through manipulation, and there is no evidence that particular individuals start cascades more often than others. Moreover, it is unclear whether a network perspective is appropriate for social navigation systems.

Putting these concerns aside, the question is whether an algorithm might be able to identify cascade behavior and discount it, leading to a more accurate depiction of the community's "best guess." The answer to this question is unclear. Algorithmic approaches require substantial amounts of data in order to be effective, which means that a system must be actively collecting data for a long time before it becomes effective. Many privacy and security decisions, however, cannot or should not be deferred, as new threats often arise quickly and do significant damage in their early stages. For such threats, community data is needed immediately rather than later.

Thus, there are difficult tradeoffs between (a) requiring users to make unaided decisions and collecting but hiding this data for a period of time in order to ensure the community data is accurate and (b) showing users limited, potentially inaccurate community data from the start, which will sometimes improve their decisions but also occasionally lead to cascades that have significant negative consequences.

Another distinct weakness of using history-based data to compute on community data is that users must maintain stable identities in order to determine which, if any, users are most likely to start or propagate cascades. This weakness requires consideration of another tradeoff: users must forfeit some measure of privacy in order to improve the accuracy of community data so that it is useful for decision making.

Using a reputation system [43] could incentivize users to forego some measure of privacy in order to build and maintain a reputation for making good decisions. The challenge for such a system is developing appropriate incentives to reward good decisions and a good reputation.

6.2 Mitigation via User Interaction

A promising—and so far unexplored—avenue of research is to mitigate cascades via user interfaces techniques. The general goal of these techniques should be to balance two competing goals: (a) enabling users to leverage community data and (b) capturing user knowledge and expertise in order to provide more accurate community data and thus mitigate informational cascades.

	Collection	User Burden	Aggregation	Expressiveness
Activity Data	Implicit	Low	Easy	Low
Ratings	Explicit	Moderate	Easy	Moderate
Free Text	Explicit	High	Hard	High
Tagging	Explicit	Moderate	Moderate	Moderate-High

Table 1. Characteristics of community data.

Today's social navigation systems afford easy use of community data but sacrifice accuracy. In contrast, imagine a user interface that affords somewhat limited use of community data in order to ensure that a system can capture some measure of users' knowledge during decision making and hence maintain the accuracy of the system's community data.

For example, instead of displaying a system's community data, a user interface could provide an additional choice labeled "go with the community decision" alongside other choices. If a user chose to go with the community decision, her decision would be the community's consensus; more importantly, her decision would not be added to the system's community data because the decision does not contribute new information to the system.

One issue with this approach is what action to take if, after a user has decided to go with the community consensus, the consensus changes to a different decision. The system could change the user's decision automatically, alert her and ask her to choose again, or do nothing. It is not clear which of these actions is best. There are risks associated with each action, and domain or contextual characteristics may also influence the best action to take.

Another option is a two-stage decision process. During the first stage, the interface would present a user with her potential choices but not show any community data. Making a choice would lead her to the second stage, where the interface would show the community data and allow her to change her decision if she wants. In this design, the user's initial decision would be included in the community data because it is uninfluenced by community data.

One drawback to this approach is that it could be gamed by users: a user could provide a random answer in the first stage and then make an authentic decision in the second stage. The most straightforward method to address this issue is to provide incentives for users to make authentic decisions in the first stage. For instance, users could be rewarded for correct or good answers in the first stage. Alternatively, research indicates that users will often make an effort to contribute to an online community if they think they have unique information to contribute [35]; a system that appeals to this motivation may encourage users to answer authentically in the first stage.

Of course, these approaches are quite rudimentary and rigid, and it is unclear whether users would accept and acclimate to more restricted and less straightforward uses of community data. However, they demonstrate the potential of an informational cascades perspective to inform the design of novel interfaces for social navigation applied to privacy and security management.

It is also worthwhile to consider how different types of community data impact the frequency of cascades. Table 1 characterizes four popular types of community data—activity or behavioral data, ratings, free text, and tagging—along four dimensions: (a) whether the collection of data require explicit

actions by users; (b) the degree of user burden in collecting the data; (c) the difficulty in aggregating the information; and (d) the *expressiveness* of the data.

We use the notion of expressiveness to characterize how much information the data type conveys to users; more expressive data conveys more information and thus is easier to understand and use. We can also draw a correlation between the expressiveness of a data type and the likelihood of informational cascades occurring: the more expressive data is, the less likely informational cascades are to occur because it is easier to understand why a user made a particular decision. This is an important correlation.

Characterizing community data types by their level of expressiveness helps explain our findings from Acumen and Bonfire. The cascades that occurred in Acumen are partially a result of its use of activity data. Bonfire's use of both activity data and tagging was well received because those data types complement each other. Activity data is simple and always present, and tagging can complement the activity data by providing a more expressive form of data, albeit at the cost of an increased burden on users.

What can be learned from this characterization of community data is that there are tradeoffs in choosing to use different types of community data. Activity data and free text lie on opposite ends of a spectrum in which the tradeoff is between ease of collection & aggregation and expressiveness & cascade mitigation. Activity data is very easy to collect and aggregate but has very low expressiveness and hence is likely to cause more cascades. In contrast, free text is difficult to collect because it places a high burden on users and is hard to aggregate, but it is very expressive and is less likely to lead to cascades. Ratings and tagging occupy the middle of this spectrum, and the difficultly in collecting and aggregating these data types is commensurate with their expressiveness and likelihood of preventing cascades.

Another tradeoff to consider when choosing the types of community data to use in a social navigation system for privacy or security management is users' motivation. The higher the user burden that a system places on users, the more motivation is needed for users to contribute data. Thus, it is important to choose a community data type that matches users' motivation. There are many potential methods to motivate users, including direct payment, reputation building, game playing, and public service.

7. FUTURE WORK AND CONCLUSION

The concept of mitigating cascades in social navigation systems for privacy and security management is powerful, and further development of the cascades concept can help clarify its scope and utility. One development path is quantifying the effect of cascades on the accuracy of Acumen and Bonfire's community data. We anticipate using informational cascades experiments [2] as a basis for performing experiments on Acumen and Bonfire to evaluate how often and under what conditions cascades form in each system. We are especially interested in quantifying the relationship between different types of community data and the propensity of cascades to form.

Another focus of future work is exploring how the surrounding sociotechnical system impacts the use and utility of a social navigation system for privacy and security management. We would like to investigate how the features of a user community affect a social navigation system. Often in digital privacy and security management, the level of expertise is uniformly low for a social navigation system's user community; we have documented how this level of expertise affects the system's use and, when cascades occur, misuse. However, how does a system's use and utility change if its user community is composed of both experts and novices, making the community's distribution of expertise bimodal? And what if the distribution is skewed slightly or markedly toward either experts or novices?

Another feature of the surrounding sociotechnical system that will impact a system's use is the outcome characteristics of a domain, such as the number of acceptable true and false positives, true and false negatives, and the perceived and real consequences of each outcome. We expect to see different usage patterns of social navigation systems based on outcome characteristics of different privacy and security management activities. In fact, psychological research indicates that both task difficulty and task importance play a role when using and interpreting others' behavior to make decisions [5].

For example, imagine that a recent computer virus renders a computer useless shortly after infecting it. If users are aware of this virus and its behavior, users are likely to perceive the cost of a virus to be quite high. Given this belief structure, users may employ community data differently when making a firewall management decision as compared to when they perceive the cost of a virus to be low.

We anticipate that this research trajectory will provide insight into the tasks and circumstances—including user beliefs and perceptions—in which social navigation systems are useful for privacy and security management.

In closing, we began this paper by discussing lessons learned from Acumen and Bonfire, two systems that employ social navigation to support privacy and security management. A primary focus in both systems is to ensure the system's data represents the community's "best guess" and not skewed by herding. Based on (i) our experiences with Acumen and Bonfire and (ii) our application of informational cascades research to social navigation systems for privacy and security management, we have argued that addressing informational cascades is an important challenge for social navigation systems applied to end-user privacy and security management.

Cascades are especially likely to occur in social navigation systems for privacy and security management because (a) there are many objective decisions in privacy and security management and (b) users often have limited expertise in managing their privacy and security. We discussed how algorithmic approaches might be used to mitigate informational cascades to social navigation systems applied to privacy and security management. Given the weaknesses of algorithmic approaches to mitigation, however, we introduced the notion of employing user interaction to mitigate cascades and argued that it is a promising approach. Both approaches present tradeoffs for designers, and these tradeoffs are grounded in features of a system's user community and larger sociotechnical system.

8. REFERENCES

[1] Ackerman, M., Cranor, L. and Reagle, J. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences *1999 ACM Conference on Electronic Commerce*, 1999, 1-8.

[2] Anderson, L.R. and Holt, C.A. Information Cascade Experiments. in Plott, C. and Smith, V. eds. *The Handbook of Results in Experimental Economics*, 2006.

[3] Bandura, A. *Social Learning Theory*. General Learning Press, 1977.

[4] Banerjee, A. A Simple Model of Herd Behavior. *Quarterly Journal of Economics*, *107* (3). 797-818.

[5] Baron, R.S., Vandello, J.A. and Brunsman, B. The forgotten variable in conformity research: Impact of task importance on social influence. *Journal of Personality and Social Psychology*, *71*. 915-927.

[6] Bikhchandani, S., Hirshleifer, D. and Welch, I. A Theory of Fads, Fashion, Custom, and Cultural Change as Informational Cascades. *Journal of Political Economy*, *100* (5). 992-1026.

[7] Cosley, D., Lam, S.K., Albert, I., Konstan, J. and Riedl, J., Is Seeing Believing? How Recommender Systems Influence Users' Opinions. in *2003 ACM Conference on Human Factors in Computing*, (2003), ACM Press, 585-592.

[8] Cranor, L. *Web Privacy with P3P*. O'Reilly, 2002.

[9] Cranor, L. What do they "indicate?": evaluating security and privacy indicators. *Interactions*, *13* (3). 45-47.

[10] Deutsch, M. and Gerard, H.B. A Study of Normative and Informational Social Influences Upon Individual Judgment. *Journal of Abnormal and Social Psychology*, *59*. 204-209.

[11] Devenow, A. and Welch, I. Rational Herding in Financial Economics. *European Economic Review*, *40* (3-5). 603-615.

[12] DiGioia, P. and Dourish, P., Social navigation as a model for usable security. in *2005 Symposium on Usable Privacy and Security*, (2005), 101-108.

[13] Domingos, P. and Richardson, M., Mining the network value of customers. in *The seventh ACM SIGKDD international conference on Knowledge discovery and data mining (KDD 2001)*, (2001), ACM Press, 57-66.

[14] Dourish, P. and Chalmers, M., Running Out of Space: Models of Information Navigation. in *1994 Conference on Human-Computer Interaction*, (1994), (Short paper).

[15] Dourish, P., Edwards, W.K., LaMarca, A., Lamping, J., Peterson, K., Salisbury, M., Terry, D.B. and Thorton, J. Extending document management systems with user-specific active properties. *ACM Transactions on Information Systems (TOIS)*, *18* (2). 140-170.

[16] Dourish, P., Grinter, R., Delgado de la Flor, J. and Joseph, M. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing*, *8* (6). 391-401.

[17] Edwards, W.K., Poole, E.S. and Stoll, J., Security Automation Considered Harmful? in *Proceedings of the IEEE New Security Paradigms Workshop 2007*, (White Mountain, New Hampshire, 2007).

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

[19] Friedman, B., Howe, D. and Felten, E., Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. in *35th Hawaii International Conference on System Sciences*, (2002), 247 (See CD-ROM for full paper).

[20] Goecks, J. and Mynatt, E.D., Supporting Privacy Management via Community Experience and Expertise. in *2005 Conference on Communities and Technologies*, (2005), 397-418.

[21] Grebe, T., Schmid, J. and Stiehler, A. Do individuals recognize cascade behavior of others? – An experimental study *Journal of Economic Psychology*, *29* (2). 197-209.

[22] Gross, J. and Rosson, M.B., Looking for Trouble: Understanding End-User Security Management in *2007 Computer Human Interaction for the Management of Information Technology*, (2007), ACM Press, 10.

[23] Harris, I. Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits, 2003.

[24] Herzog, A. and Shahmehri, N., Usability and Security of Personal Firewalls. in *2007 International Information Security Conference*, (2007), 37-48.

[25] Herzog, A. and Shahmehri, N. User Help Techniques for Usable Security *2007 Computer Human Interaction for the Management of Information Technology*, ACM Press, 2007, 11.

[26] Hill, W., Hollan, J., Wroblewski, D. and McCandless, T., Edit Wear and Read Wear. in *1992 Conference on Human Factors in Computing*, (1992), 3-9.

[27] Höök, K., Benyon, D. and Munro, A.J. *Designing Information Systems: The Social Navigation Approach*. Springer, 2003.

[28] Horrigan, J. Wireless Internet Access; A Pew Internet & American Life Project Report, 2007.

[29] Huberman, B. *The Laws of the Web: Patterns in the Ecology of Information*. MIT Press, 2001.

[30] InsightExpress. InsightExpress Study Sheds New Light on Cookie Deletion: Misperceptions About Cookies Continue, But Deletion Is Easier Said Than Done, 2007.

[31] Jensen, C. and Potts, C. Privacy Policies as Decision-Making Tools: A Usability Evaluation of Online Privacy Notices *2004 ACM Conference on Human Factors in Computing (CHI 2004)*, ACM, 2004, 471-478.

[32] Jensen, C. and Potts, C. Privacy practices of Internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63* (1-2). 203-227.

[33] Lampe, C. and Resnick, P., Slash(dot) and Burn: Distributed Moderation in a Large Online Conversation Space. in *2004 SIGCHI conference on Human factors in computing systems*, (2004), ACM Press, 543-550.

[34] Leskovec, J., Krause, A., Guestrin, C., Faloutsos, C., VanBriesen, J. and Gruhl, D., Cost-effective outbreak detection in networks. in *13th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD 2007)*, (2007), ACM, 420-429.

[35] Ludford, P.J., Cosley, D., Frankowski, D. and Terveen, L.G. Think different: increasing online community participation using uniqueness and group dissimilarity *2004 SIGCHI*

conference on Human factors in computing systems, ACM Press, 2004, 631-638.

[36] McNee, S., Kapoor, N. and Konstan, J.A., Don't Look Stupid: Avoiding Pitfalls when Recommending Research Papers. in *2006 Conference on Computer-Support Cooperative Work (CSCW 2006)*, (2006), 171-180.

[37] Millett, L., B., F. and Felten, E., Cookies and Web Browser Design: Toward Realizing Informed Consent Online. in *2001 Conference on Human Factors in Computing (CHI)*, (2001), 46-52.

[38] Paine, C., Reips, U., Stieger, S., Joinson, A. and Buchanan, T. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, *65* (6). 526-536.

[39] Palen, L. and Dourish, P., Unpacking "Privacy" for a Networked World. in *2003 Conference on Human Factors in Computing*, (2003), 129-136.

[40] Pew Internet & American Life Project. Report: Home Broadband Adoption 2006, 2006.

[41] Pew Internet & American Life Project. Spyware, The threat of unwanted software programs is changing the way people use the Internet; The Pew Internet & American Life Project Report, 2005.

[42] Pew Internet & American Life Project. The Broadband Difference: How online Americans' behavior changes with high-speed Internet connections at home, 2004.

[43] Resnick, P., Kuwabara, K., Zeckhauser, R. and Friedman, E. Reputation Systems. *Communications of the ACM*, *43* (12). 45-48.

[44] Resnick, P., Neophytos, I., Suchak, M., Bergstrom, P. and Riedl, J., GroupLens: an open architecture for collaborative filtering of netnews. in *1994 Conference on Computer-Supported Cooperative Work*, (1994), 175-186.

[45] Resnick, P. and Sami, R., The influence limiter: provably manipulation-resistant recommender systems. in *2007 ACM Conference on Recommender Systems*, (2007), ACM, 25-32.

[46] Schneier, B. *Secrets and Lies : Digital Security in a Networked World*. Wiley, 2004.

[47] Shilad, S., Shyong, K.L., Rashid, A.M., Cosley, D., Frankowski, D., Osterhouse, J., Harper, F.M. and Riedl, J., Tagging, communities, vocabulary, evolution. in *2006 ACM Conference on Computer-Supported Cooperative Work*, (2006), ACM Press, 181-190.

[48] Svensson, M., Höök, K., Laaksolahti, J. and Waern, A., Social Navigation of Food Recipes. in *2001 Conference on Human Factors in Computing*, (2001), 341-348.

[49] Taubes, G. *Good Calories, Bad Calories: Challenging the Conventional Wisdom on Diet, Weight Control, and Disease*. Knopf, 2007. Turow, J. Americans and Online Privacy: The System is Broken, 2003.

[50] Turow, J. Americans and Online Privacy: The System is Broken, 2003.

[51] Walden, E.A. and Browne, G.J., Information Cascades in the Adoption of New Technology. in *2002 International Conference on Information Systems*, (2002), 435-443.

[52] Welch, I. Sequential Sales, Learning, and Cascades. *Journal of Finance*, *47* (2). 695-732.

[53] Wexelblat, A. and Maes, P., Footprints: History-Rich Tools for Information Foraging. in *1999 Conference on Human Factors in Computing*, (1999), 270-277.

[54] Whitten, A. and Tygar, J.D. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *8th USENIX Security Symposium*, Usenix, 1999, 169-184.