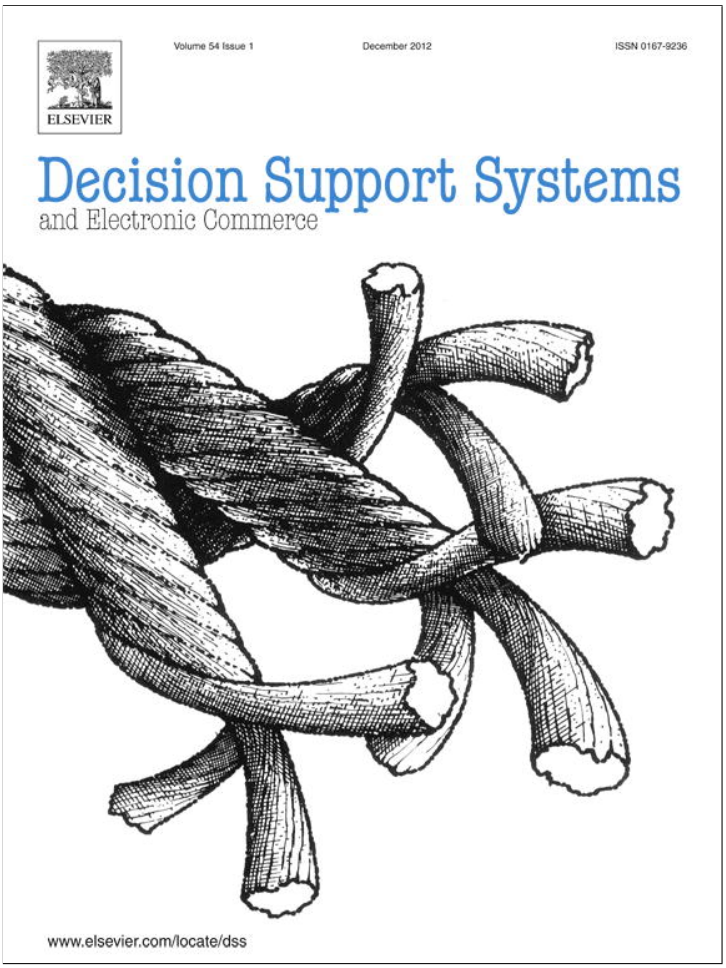

Decision Support Systems 54 (2012) 424–433

Contents lists available at SciVerse ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers

Heng Xu [a,*], Robert E. Crossler [b,1], France Bélanger [c,2]

[a] College of Information Sciences and Technology, The Pennsylvania State University, University Park, Pennsylvania, United States
[b] Department of Management and Information Systems, Mississippi State University, Mississippi State, Mississippi, United States
[c] Department of Accounting and Information Systems, Virginia Tech, Blacksburg, Virginia, United States

ARTICLE INFO

Article history:
Received 15 March 2011
Received in revised form 20 May 2012
Accepted 19 June 2012
Available online 27 June 2012

Keywords:
Privacy-by-Design (PbD)
Privacy-Enhancing Tools (PETs)
Value Sensitive Design (VSD)
Control agency
Information privacy

ABSTRACT

Privacy concern has been identified as a major factor hindering the growth of e-business. Recently, various privacy-enhancing tools (PETs) have been proposed to protect the online privacy of Internet users. However, most of these PETs have been designed using an ad hoc approach rather than a systematic design. In this paper, we present an exploratory investigation of an end-use PET using a Value Sensitive Design approach. We propose an integrated design of a Privacy Enhancing Support System (PESS) with three proposed tools, namely privacy-enhancing search feature (PESearch), privacy-enhancing control for personal data (PEControl), and privacy-enhancing review for sharing the ratings and reviews of websites' privacy practices (PEReview). This system could enhance the interactivity of Internet users' privacy experiences, increase users' control perceptions over their personal information, and reduce their privacy concerns. An empirical evaluation of PESearch, PEControl, and PEReview revealed that novices felt the most important aspect of the tools for downloading and usage intentions was its usefulness; most experts felt the tool met the design principles as specified.

1. Introduction

As Internet-based tracking and profiling technologies increasingly expand the ability for e-commerce vendors to collect, store, process and exploit personal data, privacy concern has been identified as a major factor hindering the growth of e-commerce [32]. Indeed, a Pew Internet Project survey found that 85% of adults believed it was "very important" for them to control access to their personal information [35]. The concerns center on the confidentiality of accumulated consumer personal information and potential risks that consumers experience over the possible breach of confidentiality [5].

The need to protect privacy has led to many initiatives, some behavioral and some technical. Behavioral initiatives generally include providing assurances through privacy seals [24], government regulations [58], or addressing individuals' concerns for information privacy, which have been shown to affect trust [36]. While these approaches to protecting privacy are interesting, this paper focuses on an IT artifact that provides one technical solution to the online privacy issue. This approach is in line with a recent review of the privacy literature that highlights the need for more design research in the information privacy domain [5].

Technical approaches to protect privacy result in the development and implementation of Privacy-Enhancing Tools (PETs).[3] Implementation of PETs into the design of e-commerce applications at the earliest stages offers some promise in attempts to maximize the potential of e-business. Researchers suggest that PETs would play an important role in protecting online privacy, particularly because of their ability to cross country, regulatory, and business boundaries [60]. However, among many studies designing PETs in various contexts, few systematic attempts have been made to provide an integrated framework on the design of PETs. In response to the recent call of *Privacy by Design is Essential* [20], this study is intended to systematically develop a near-complete decision support system for privacy protection called the Privacy Enhancing Support System (PESS) using a Value Sensitive Design approach. Implemented at the web browser level, PESS evaluates a website's privacy practices using three tools, i.e., a privacy-enhancing control tool for controlling user personal data (PEControl), a privacy-enhancing search feature (PESearch), and a privacy-enhancing review tool for sharing user ratings and reviews on vendors' privacy practices (PEReview). The three privacy-enhancing tools were integrated into one end-user application and embedded into browsers to provide decision support for pri-

* Corresponding author. Tel.: +1 814 867 0469.
E-mail addresses: hxu@ist.psu.edu (H. Xu), rob.crossler@msstate.edu (R.E. Crossler), belanger@vt.edu (F. Bélanger).
[1] Tel.: +1 662 325 0288.
[2] Tel.: +1 540 231 6720.

[3] When examining PETs, it is important to realize that the spectrum of systems and techniques mentioned above cover two extremes of control over PETs, with enterprise-level customer information protection at one end [27,28,70] and individual PETs at the other end [7,10,21,29,39,64]. Because it has been found that end-user PETs help reduce consumers' privacy concerns and increase consumer trust on vendors [23], we focus in this study on the design of individual PETs from the end-user perspective.

0167-9236/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2012.06.003

vacy decisions and evaluations. Following Design Science guidelines [22,37], upon implementing the PESS prototype, we conducted an empirical evaluation using a qualitative research approach.

This study is novel to the extent that existing security and privacy research in the information systems (IS) field has not systematically examined the Privacy-by-Design issues. Drawing on a Value Sensitive Design perspective, our integrated design of PETs presented in this paper offers new insights to evaluate privacy protections by users. The results should be of interest to e-business researchers and practitioners alike, as well as privacy advocates, and regulatory bodies.

2. Literature Review

According to a Pew Research Center study [35], individuals are becoming more concerned with their presence online, but less than 3% of individuals are actively protecting their online presence. Studies regularly show that many factors affect an individual's concerns for information privacy [67], which ultimately affect their willingness to participate in transactions or share information online [32,68]. In response to privacy threats, researchers and practitioners have explored various behavioral and technological approaches for privacy protection at different levels.

In tackling security attacks and privacy threats, both web service providers and web browser vendors have made significant efforts [53]. As a communication doorway to the Internet for users, a web browser plays a critical role in mediating interaction between end-users and web pages. This crucial position of the web browser facilitates its role in informing and warning end-users of security and privacy risks directly. In addition, the market of the web browser is relatively centralized – Internet Explorer (IE) and Firefox account for more than 80% of the market [62]. Such concentrated market helps push and deploy standardized web security and privacy interfaces and features [55]. However, based on our literature review, we find that the context of web browsing systems is still under development in the field of IS research. We believe that gaining an understanding of privacy protection approaches in this context is particularly important because it contains features with which end-users would interact in everyday use. Consequently, we unfold our discussion of prior studies encompassing privacy protection features by two levels: i) websites, and ii) web browsers.

2.1. Privacy-enhancing features at the web server level

Privacy policies describe an organization's privacy-related practices, which provide an explanation and claim of the organization on when and what to collect, and how personal information will be used and stored. In the privacy literature, the effect of the availability of a privacy policy on fostering consumers' information disclosure appears inconsistent. On one hand, it has been suggested that the presence of a privacy policy effectively enhances consumers' perceptions of procedural fairness and thus increases their intention to transact online or disclose personal information [13,44]. On the other hand, other studies identify various problems of privacy policies. As Antón et al. [3] pointed out, most privacy policies lack readability and are hard to understand, and they differ greatly from site to site due to the lack of industrial standards. Further, users may not be willing to spend time reading the privacy policies of websites. Even when end-users would read a privacy policy, they have no means to identify the inconsistency between the privacy policy and the website's real privacy practices [26,48].

The Platform for Privacy Preferences (P3P) created by the World Wide Web Consortium was developed to create a machine readable, common vocabulary for identifying privacy practices [10]. P3P allows users to setup a set of privacy preferences that are then compared with a website's privacy policy and provides feedback to the user that allows them to make better decisions on what type of personal information to release [8,49]. However, a technical report prepared for the FTC studying the use of P3P found that, in general, the error rate for P3P implementation was unacceptably high, many policies were out of date, and that "it may be necessary to explore the possibilities of third-party P3P policy certification, auditing, or other measures to ensure that P3P policies are trustworthy" [11].

Privacy seals are programs that businesses can participate in to show their commitment to security (e.g., Verisign), trustworthiness (e.g., webtrust.org), or privacy (e.g., TRUSTe). Once joining the program, the business is allowed to post the third-party "seal" claiming their membership and participation. Privacy seals are usually displayed on websites to help both consumers click with confidence and online companies to promote their privacy policies online [52]. The availability of a privacy seal has been found to positively associate with a consumer's trust belief in a website [51], leading to more favorable perception toward the website's privacy policy [45]. However, a number of privacy studies revealed insufficient consumer trust toward third-party privacy seals. For example, in a study [45] reviewing 60 high-traffic websites, Miyazaki and Krishnamurthy found no support for the proposition that a firm's participation in a seal program is a positive indicator of better privacy practices (Larose and Rifon [30] and Bélanger et al. [6] had similar findings).

2.2. Privacy-enhancing tools at the web browser level

Security toolbars [64], *active and passive warnings* provided by the web browser [16] and *Extended Validation (EV) certificates* [54] are privacy and security indicators provided by web browsers. These features usually indicate an encrypted connection to a particular website, through various cues such as the *https* prefix in a URL and the padlock icon in the browser chrome. A number of studies have examined effectiveness of these web browser indicators on promoting end-users' privacy and security awareness. For example, Whalen & Inkpen [63] collected eye-tracking data to study users' attention paid to browser cues. Results from this study indicate that the padlock is commonly viewed without interaction. Moreover, Sobey et al. [54] explored user reactions to EV certificate indicators and their eye-tracking data showed that all users did not notice the design of EV certificate in Firefox.

Net Trust [21], designed as a toolbar for web browsers, is a trust evaluation system that helps users evaluate whether a website is trustworthy by combining their own trusted sources of information with the trusted sources of information provided by their social network. A recommendation on the trustworthiness of a website is then made to them based on the results of their social networks' ratings. However, the design of Net Trust focused on the exchange of post-use experiences, which failed to empower users with control of their privacy during an interaction with a website.

A number of *privacy control features* (e.g., privacy controls, cookie controls, and object controls) have been implemented at the browser level by most web browsers. For example, the four major browsers (Internet Explorer, Firefox, Chrome and Safari) recently added private browsing modes to their user interfaces. This feature assures that sites visited while browsing in private mode should leave no trace on users' computers. Aggarwal et al. [1] conducted a study to evaluate the effectiveness of these privacy control features including numerous add-ons (e.g., CookieSafe for cookie controls in Firefox, and AdBlock Plus for banner advertisements in Firefox). They pointed out that flaws and vulnerabilities exist in terms of how these browsers and add-ons approach protecting privacy and concluded that browsers sometimes leak information when in private mode.

Recently, Microsoft introduced in Internet Explorer 9 a customizable *Tracking Protection List (TPL) feature* for privacy protection [38,39]. TPLs are lists of domains, subdomains, specific urls, and/or specific files that are created by privacy advocates or user communities, which support both *Block* lists and *Allow* lists. A domain in an

Allow TPL means that it can be visited from anywhere. For a domain in a *Block* TPL, the browser will only allow visits to that domain if a user specifically clicks on a link, or from that domain itself. That is to say, no third-party visits will be allowed to that specific domain, which will block third-party tracking from that domain. However, TPL is an opt-in feature and these lists will not be included and maintained by the browser but users have to create their own lists or download ready-made ones from privacy advocates such as TRUSTe [59] or PrivacyChoice [47]. Such an opt-in approach may be problematic because it shifts the responsibilities to average users. Since users usually regard their online activities as primary tasks (e.g. web browsing, checking email, online shopping, and online banking), privacy tasks such as maintaining the TPL list are not supposed to be so obtrusive that users may feel annoyed or overly-burdened by them.

At a more basic level, browsers provide the ability to specify the level of privacy a user wants to use from low to high. The privacy setting level will determine how much information is released through cookies. If the level is set too high, then it can prevent some webpages from displaying properly [40]. If it is set too low, then it allows private information to be unknowingly released to websites.

2.3. Summary

As discussed above, earlier studies on current privacy-enhancing features reveal that there exist three limitations in the literature. First, most privacy-enhancing features at the web site level cannot help users evaluate whether a particular site implements its privacy policy as it claims [3,11,17,26,48]. However, we believe that privacy-enhancing features at the web browser level could address this issue. For example, Net Trust [21] can verify the site's privacy practices to some extent because it allows users to review (by both numbered rating and comments) the interaction experience with a particular website, and share the reviews with other users via a linked social network. User reviews, therefore, could become one reliable source for peers to make inferences about the trustworthiness of a vendor. Second, most PETs at the browser level do not allow users to view their transaction histories (e.g. at websites such as ebay.com and amazon.com), to set the length of a log period kept by a particular vendor, or to check those third parties which have access to the user history logs [1,40]. Third, current PETs at the browser level have been designed using an ad hoc approach, and few systematic attempts have been made to provide an integrated design of PETs. Therefore, there is a lack of an integrated solution that can provide an easy-to-use system with various PETs. To address these limitations, we adopt a systematic approach to design the PESS system using the Value Sensitive Design approach.

3. Privacy-Enhancing Support System (PESS)

3.1. Value Sensitive Design

Value Sensitive Design (VSD) is an approach to the design of information systems that accounts for human values throughout the design process [18,19]. Example work in VSD includes security features of web browsers [43], groupware systems to support knowledge sharing [42], and kids' online safety protection [14,66]. We adopted a VSD approach for this study because this approach particularly emphasized values with moral import such as privacy and trust. VSD adopts a tripartite approach by iterating on three types of investigations: *conceptual*, *empirical*, and *technical* investigations [18,19]. Central to its tripartite methodology [18,19], conceptual investigations comprise theoretically informed analyses of constructs and issues under investigation; technical investigations focus on the features, architecture and infrastructure of the technology under examination and development; and empirical investigations focus on the actual or potential users' responses to the technical artifact and contexts-of-use.

In this study, we present the design of our Privacy-Enhancing Support System (PESS), which followed the steps recommended in the VSD approach. The first phase of the VSD approach is a conceptual investigation of the concepts of interest. The second phase includes a technical investigation of PETs for web browsers, followed by the empirical investigation of the user responses to the designed prototype.

3.2. Phase I: conceptual investigation of end-user PETs

One very important perspective views privacy to be related to the *control* of personal information. A number of privacy theorists have put emphasis on the concept of *control* when defining privacy. For example, Stone et al. [57] viewed privacy as the ability of the individual to control personal information about one's self. This control perspective of privacy is also found in prior privacy studies, which posited that loss of control over disclosure and use of personal information is central to the notion of invasion of privacy [15]. Previous privacy research has revealed that individuals will have lower levels of privacy concerns when they have a greater sense that they can control the disclosure and subsequent use of their personal information [12,13,65]. Therefore, it seems that incorporating the notion of *control* into the design of the end-user PETs is the key to alleviate users' privacy concerns.

Drawing from the extant IS literature on security and psychological control theories, two theories related to control are applicable in the context of this research: the technology threat avoidance theory [33] and Yamaguchi's control agency theory [69]. The technology threat avoidance theory [33] suggests that, after users become aware of a threat (e.g., privacy breach), they would assess the degree to which the threat can be avoided by adopting technological safeguards. An important assessment that users need to make in this process is to determine how much control they have over the specific threat or how avoidable the threat can be [33]. A user's perception that adopting a privacy safeguard mechanism (e.g., PESS) will help protect online privacy enhances his or her motivation to cope with the threat. This theoretical approach provides justification for the expectation that the PESS developed in this research can motivate users to protect their online privacy.

Yamaguchi's control agency theory [69] posits that there are three types of controls based on three types of control agents: 1) *personal control*, in which oneself acts as the control agent, 2) *proxy control*, in which powerful others act as the control agent, and 3) *collective control*, in which the collective acts as the control agent. Following Yamaguchi's control agency theory [69], we propose three design principles, which serve as the design guidelines to empower different types of privacy control in the PESS.

People who value autonomy would prefer exercising direct *personal control* as they "would especially feel themselves more self-efficacious when their agency is made explicit (p.226)" [69]. For this type of control, users act as control agents to exercise direct personal control over when and how their personal information is released for use by a website [65]. Thus, we propose:

- *Design Principle #1*: Privacy-enhancing tools should be designed to empower users with personal control where users themselves act as the control agents to directly control over when and where their personal information is released for use during the conduct of online transactions at a specific website.

However, when the employment of personal control is neither obtainable nor encouraged, individuals might well give up their direct control preferences and seek "security in proxy control (p.142)" [4]. *Proxy control* is defined as an attempt to align oneself with a powerful force in order to gain control through powerful others [69]. When users perceive that they lack the necessary skills, resources and

power to directly control their personal information disclosed for online transactions, they may reform their decisions by considering the availability of powerful others (e.g., TRUSTe) who can act on behalf of them to protect their online privacy [65]. Hence, the design of privacy-enhancing tools should easily indicate the availability of users' proxy control – whether the structure like TRUSTe is in place to assure that the online transaction environment is safe and secure.

- *Design Principle #2*: Privacy-enhancing tools should be designed to indicate the availability of proxy control where powerful forces (e.g., industry self-regulators such as TRUSTe) act as the control agents for users to exercise proxy control over their personal information.

The third type of control is *collective control* in which an individual attempts to control the environment as a member of a group or collective [69]. As demonstrated by the Net Trust [21], user reviews shared via a linked social network could become one reliable source for peers to make inferences about the trustworthiness of a website in terms of its privacy practices. Therefore, we propose:

- *Design Principle #3*: Privacy-enhancing tools should be designed to empower users with collective control where users act as a member of a group to exercise collective control over their personal information.

3.3. Phase II: technical investigation of end-user PETs

Following the philosophy of Value Sensitive Design, the above conceptual investigations can now be employed to help structure the first iteration of a technical investigation. Specifically, we designed three privacy-enhancing tools to empower users with personal control, proxy control and collective control over their personal information. Collectively, we use PE*tools to refer to the three privacy-enhancing tools – PEControl, PESearch and PEReview.

3.3.1. Design of PEControl

Following design principle #1, we designed a tool named PEControl to empower users with direct personal control over their personal information. PEControl has the following design features:

1. *Genericity*. We designed the instrument of privacy control as Web services [2] running at a vendor's web server. These services receive and process user requests for privacy control. Results of request processing are then sent back to requestors. Vendors publish these services using Web Service Description Language (WSDL) [61]. Whenever users visit an online vendor, the client-end of the tool – PEControl agent retrieves and interprets the vendor's WSDL file and dynamically builds a user-interface for privacy control at this website. The PEControl Agent subsequently interacts with users, sends user control request to the vendor's web services and displays service responses to the user. The use of WSDL allows vendors to dynamically add, modify or remove privacy control mechanisms that are implemented as Web services compliant to the WSDL protocols.
2. *Progressive configuration*. The PEControl agent allows privacy control settings to be configured in a progressive manner. It is designed as a plug-in to a Web browser, enabling users to check or change privacy settings without leaving the current session with the vendor. Thus, inexperienced users can use the PEControl agent to preview the effect of changes to their privacy settings without actually setting them during a single visit to a website. Gradually, they get familiar with the system, understand their privacy needs, and increasingly fine-tune their privacy settings. With increasing experience with the tool, the vendors, and overall browsing, users can become more adept at selecting the proper privacy preferences for themselves.
3. *Coarse-grained and fine-grained control*. To avoid demanding a fair amount of user effort on the privacy option settings, the PEControl Agent is designed to provide three top-level control features:
   a) Minimum data release, which will request the vendor to turn off all unnecessary data collection and to shorten the data-keeping period to the minimum necessary for the current session; data sharing with third parties will not be allowed under the request of minimum data release;
   b) Restore to vendor-default privacy settings; and
   c) Maximum data release.

In addition to these coarse-grained controls, the PEControl agent also provides detailed configurations for privacy settings. More implementation details will be discussed in Section 3.3.4.

3.3.2. Design of PESearch

Following design principle #2, PESearch is designed to utilize a proxy to provide a user with information about a website's privacy practices prior to the user's visit. PESearch maintains a store of online vendors' ratings of privacy practice and employs web crawlers [9] to update the store frequently. PESearch has the following unique design features:

1. *Providing search pointers to multiple information sources*. PESearch not only uses a vendor's privacy policy as one information source; it also looks for third-party trust seals (e.g., TRUSTe) and user ratings on the vendor's privacy practices. These sources of information are used to calculate a website's aggregated privacy rating, which is then used to rank search results. Besides searching over the multiple information sources, the display of search results also provides privacy indicators for individual information source. Users could learn from these individual privacy indicators about a vendor's privacy practices.
2. *Verifying information source when possible*. Users should be provided with verifiable guarantees [25]. PESearch verifies third-party privacy or trust seals stated in a vendor's privacy policy by automatically checking the validity of the seal through the website of the seal-granting organization. Placing invalid or expired privacy seals will cause PESearch to give a *Red Alert* privacy indicator on the search result page. Moreover, PESearch employs some heuristics to detect the vendor's potential opportunistic behaviors. For example, when PESearch finds a website's P3P privacy policy has no dispute mediation clause, a *Red Alert* privacy indicator will be displayed for this website.

Moreover, *users' prior privacy related knowledge and prior online privacy experience* are also considered in the design of PESearch. Inexperienced users might simply want the PESearch to search by online vendors' privacy practices without providing any privacy preferences, because preferences are hard to get right at a time when users first use a system [23,34]. In contrast, experienced users might want to search with certain privacy preferences. Based on these design considerations, PESearch is designed to work in three modes: 1) simple search mode, in which privacy rating is used to re-order search results, and no user preference is required; 2) advanced and speedy search mode, in which users can search online vendors against a pre-defined privacy preference; and 3) advanced search mode in which users can fully customize privacy preferences used for search.

3.3.3. Design of PEReview

Following design principle #3, PEReview is designed to empower users with collective control where they act as a member of a group to collectively control their personal information. Similar to Net Trust, PEReview "embeds social context in web-based trust decisions by combining individual histories, social networks, and explicit ratings (p.1)" [21]. PEReview inherits Net Trust's merit of avoiding the risk of a vendor's opportunistic behaviors in the trust-decision

process. Users' trusted sources of information (e.g., friends' feedback) are used to evaluate the trustworthiness of a vendor. PEReview extends Net Trust with the following two additional design values:

1. *Capturing user reviews in user-searchable formats*. In PEReview, users can provide privacy rating and text comments to an online vendor's online and offline channels. Privacy ratings of a vendor can be made as an overall score (a singular numerical value), and/or on specific elements of privacy practices. Thus, privacy rating is represented in PEReview as both a singular value (used in PESearch's simple search mode), and as a multi-dimensional vector (used in PESearch's advanced search modes where the distance between user preference vector and privacy rating vector is calculated to rank search results).
2. *Supporting reviews of online vendors' privacy practices in an offline channel*. Users can rate and make comments to the privacy practice observed from a vendor's online channel, or offline channel. This design is useful for monitoring the privacy practice of those online e-commerce vendors which also have a physical presence and offline transaction channels [56]. The reason for explicit differentiation of offline channels versus online channels is to allow more specific search in online channel(s) only, in offline channel(s) only, or a mix of both.

3.3.4. Prototype development

We developed a prototype to integrate the aforementioned three privacy-enhancing tools. The prototype is designed as an add-on toolbar for Web browsers such as Internet Explorer and Mozilla Firefox. This toolbar is named as PE*ToolSet. Fig. 1 is an overview of the toolbar.

On the PE*ToolSet toolbar, there are the two frequently accessed privacy control functions. The left one is *View My Data@Site*, which displays the types of personal data collected by the vendor of the current website in a new window. The right one is *Control My Data@Site*, which contains three shortcuts to the top-level privacy controls (see Fig. 2a), with additional information available to users. The rest of the control functions are embedded in the *More!* dropdown menu, which include three functions: 1) view access log, 2) report data error, and 3) additional site-specific privacy controls (see Fig. 2b).

The search box implements the PESearch's simple search feature. Advanced search modes are placed in the *Search* dropdown menu as illustrated in Fig. 3. Fig. 4a and b illustrate the use of PEReview. Overall rating, specific rating on some particular elements of privacy practice, and textual comments are provided in the *Rate@Site* dropdown menu. Live reviews made by other users from the buddy list are periodically pushed to PEReview. Fig. 5a shows the summary list of buddy reviews and Fig. 5b shows the details of one buddy review.

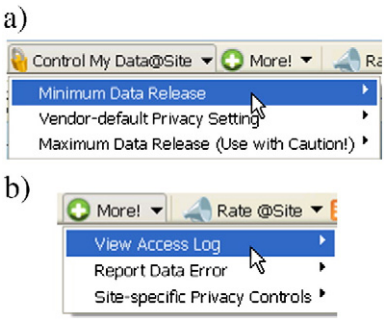

Fig. 2. a) Top-level privacy control functions in *Control My Data@Site* dropdown menu. b) Additional privacy control functions in *More!* dropdown menu.

3.4. Phase III: evaluation of end-user PETs

The user responses to the PE*Toolset were evaluated utilizing a qualitative methodology. The intent of this approach was to make sure that the design principles identified in the conceptual phase were sufficiently met in the opinion of the target user population. We regarded protecting one's online privacy as a sensitive topic. Consequently, there may be social implications to responses users give. When collecting data about sensitive topics (e.g., asking one's privacy perceptions), it is appropriate to utilize open-ended questions to allow respondents to express themselves in a way that they do not feel threatened [31]. Doing so allows respondents to say as much or as little as they would like and not be confined to a limited set of answers that are available in a Likert-type survey design.

Two separate evaluations were conducted. The first evaluation was performed by privacy experts and focused on the evaluation of the design of the tool. The questions asked were aimed at understanding whether or not the tool was designed in such a way that it met the design principles set forth prior to development. The second evaluation was performed by privacy novices and focused on an evaluation of adoption and use of the designed tool. The questions asked were aimed at determining whether or not individuals would download and use this tool if it were available to them.

The data collected was coded based on a set of codes developed from the questions asked, as well as information received from the responses [41]. Initially, two coders coded seven responses and their results were compared. Where there were differences in the codes, the researchers tried to come to a consensus. When this was not possible, a third researcher provided a decision. After this, the remainder of the responses were coded. For the coding of the expert responses, there was a Cohen's Kappa of .70, and for the novice responses, there was a Cohen's Kappa of .72, which suggests a high level of agreement.

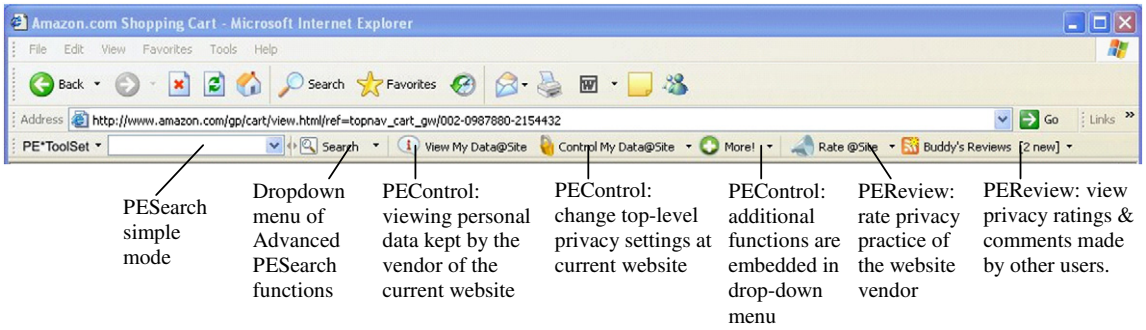

Fig. 1. The current design of the PE*ToolSet toolbar.

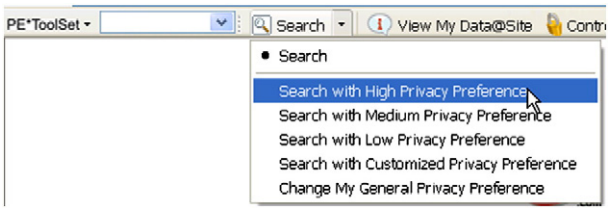

Fig. 3. Advanced PESearch functions in *Search!* dropdown menu.

3.4.1. Experts

Eighteen experts were interviewed and asked if they felt the design of the PESS met the design principles laid out prior to evaluation as well as what, if any, factors should be given more considerations in future versions of the system. Experts were individuals enrolled in a master's level class who had significant IT experience and training prior to the course, and were trained during the course of the program on the intricacies of security and privacy management. Thirteen of the 18 experts felt that the PESS met the design principles as specified.[4] In addition, we asked experts what features could be improved in future design; these results were presented in Fig. 6. Only those suggestions that were mentioned by more than one expert are presented here. Those items that were only mentioned once include access, collective actions, confidentiality, ease of use, enforcement, feedback, granularity, notice, unauthorized access, user error, and user notification.

The response that arose most often in evaluation by the experts is that usability is an important design consideration in future privacy-enhancing tools. A number of suggestions for future improvements to the design of this tool were provided, such as continuous reminders of the importance of privacy and the tool should be something that non-technology savvy users should be able to easily use.

> *"The program assumes that the user is constantly on the lookout for their privacy, which may be the case in the short term, but long term usage patterns tend to indicate that people get lazy, and some inconvenience is necessary to remind them to maintain their privacy (see: User Access Control in windows Vista). While the user is "empowered" by the abundance of information, without constant reminders and warnings from the program, the user will eventually simply forget."*

> *"Many people are not technology savvy so the privacy software or program should be easy to use for first time user. Also adding to this thought, it should be simple and appropriate."*

Another suggested issue in the design that arose was the lack of legal authority that industry self-regulators have.

> *"Having industry self-regulators acting as control agents for users to exercise proxy control is not sufficient for privacy concerns. Industry regulators do not have any legitimate power to control the privacy of users."*

Experts also indicated that once an individual provides data to a company, properly securing the data becomes paramount.

> *"However, simply being able to choose whether or not your data is released is not enough. For example, a user has a certain expectation of integrity and security. That is, users have a right to know that the information they release to a particular company is going to be stored using a secure process (encryption, secure sockets for transfer of data, etc.)."*

While we agree with these latter two assessments about what is lacking with this system, there is no way to implement an adequate solution to take things to this level without (1) getting legislative involvement, and (2) gaining permission to access and monitor the storage of private data. Neither of these approaches is feasible in the design of such a system.

3.4.2. Novices

Novices were students with no knowledge of PET design, information privacy or security concepts beyond their own personal experiences. These students had not attended any classes related to these concepts and only had an introduction to information technology in general. Twenty-one novices participated in the evaluation. The age of the novices ranged from approximately 19 to 22 years old. There were 12 males and 9 females in the sample.

The novices indicated that the most important aspect to encourage downloading as well as a continued usage of this tool is the usefulness it provides. As can be seen from the comments below, most respondents indicated their perceived usefulness of the PET tool. Other factors identified for usage and download importance, as shown in Fig. 7, include: website warnings, social influence, security, comments from others, control, browser space, free, privacy concerns, ease of use, efficiency, and ability to rate websites.

> *"The protection of privacy on one's computer is a must in the digital age. I would initially download this privacy toolbar for its ability to specify the amount of personal data that can be released from different websites."*

> *"I would download this toolbar for more dynamic privacy controls than the basic controls provided by a web browser like Mozilla Firefox or Internet Explorer."*

> *"As long as the toolbar proved to be helpful and useful, I would continue to use it."*

> *"I would continue to use it because the internet is very vast so the more chances I would get to protect myself the better."*

The novice reviewers further stated that receiving website warnings or warnings about the information websites collect was another important feature in the design of the privacy protecting software that would both make them initially download the software as well as continue using it.

> *"I would love the PEControl item. I frequently wonder what kinds of information a website is picking up and keeping from me. For example, when I pay my bills online, some online billpays can recall your credit card number even though you didn't specifically save it in a profile - this makes me nervous."*

> *"I would continue to use it because I could help my friends out by warning them in advance of the bad sites they should avoid."*

Some interesting findings from novices were that although security and social influence were often mentioned as factors in the initial download of the PESS, they were mentioned much less frequently as factors in the continued use of the PESS.

[4] Of the five experts that felt that PESS did not meet the design principles specified, one did not actually answer the question asked, and four provided reasons why the design principles were not met that were outside of the researchers' control, such as legal enforcement (2) and potential secondary use of data (2).

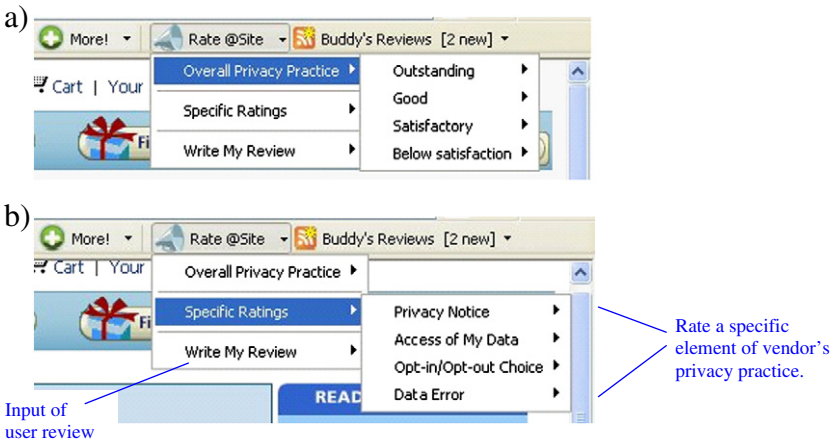

Fig. 4. a) Overall user rating on privacy practice in PEReview. b) Specific user rating and input of user review in PEReview.

"How effective this tool is in providing a secure and safe profile of me while online."

"I think initially to be persuaded to download the toolbar I would have to hear word of mouth recommendations from friends, family, or professors."

Furthermore, while control and ease of use were not regularly mentioned as factors in the download of the PESS, they were mentioned more frequently as factors in the continued usage of the PESS.

"There are many reasons to continue to use this toolbar. I have preference to set my privacy. I can change my privacy setting at any time. I have control in which data will be available to see by other people."

"If I was able to identify that I was successfully keeping my personal information private with ease of use, I would continue to use it."

In summary, the evaluations of PESS revealed that novices felt the most important aspect for downloading and usage intentions is its usefulness. The evaluation also revealed that most experts felt the tool met the design principles as specified.

4. Discussion

This study's purposes were two-fold. First, we wanted to follow a structured approach to design privacy-enhancing tools for online users. For this purpose, we used the design method of Value Sensitive Design. Second, we wanted to follow design science principles to ensure that users and experts would find the PESS usable and well designed.

The Value Sensitive Design (VSD) principles proved to be very useful is establishing clear requirements for the PET tools. We did find that some design factors, such as those that related to initial concerns, are important in gaining adoption of a given technology; however, other design factors, such as those that deal more with functionality, are important considerations for the continued use of the technology. It is surprising that IS research has not systematically examined privacy issues from the *Value Sensitive Design* perspective; this makes the present study novel. We believe that future research in information systems, more particularly in design science research, would benefit from considering the principles of VSD when designing IT artifacts. Using the groundwork laid down in this study, future research could contribute significantly to maximizing the potential of e-business.

Hevner and his colleagues suggest that IS research is at "the confluence of people, organizations, and technology [22] (p. 77)." In designing our PESS, we followed the design science principles which include: 1) Design as an Artifact (PESS including PESearch, PEControl, and PEReview), 2) Problem Relevance (the importance of protecting users' privacy), 3) Design Evaluation (the evaluation of the design artifact by novices and experts), 4) Research Contributions (the PESS, as well as a better understanding of the benefits of Value Sensitive Design), 5) Research Rigor (a review of relevant literature, the use of Value Sensitive design in establishing design requirements, and technical evaluation by two stakeholder groups), 6) Design as a Search Process (a review of relevant literature and the use of Value Sensitive Design in establishing design requirements), and 7) Communication of Research (presentation of our PESS to user communities and description of the PESS provided in this paper) [22].

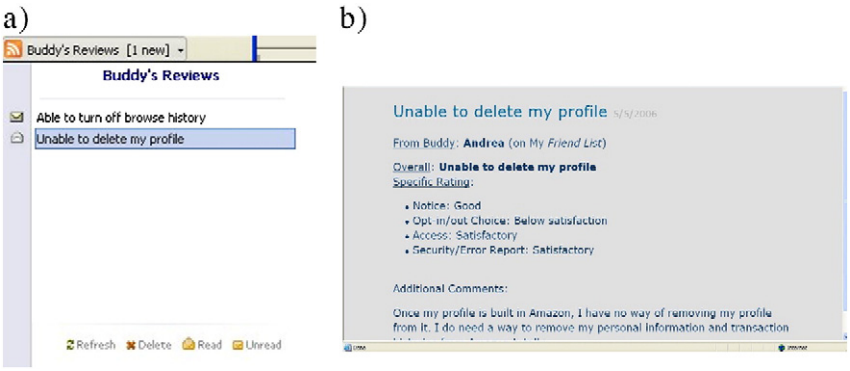

Fig. 5. a) Summary view of buddy's privacy review in PEReview. b) Detailed view of a buddy's privacy review in PEReview.

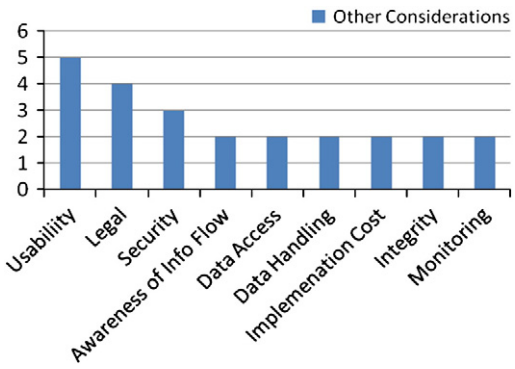

Fig. 6. Technical evaluation: expert suggestions for improvements.

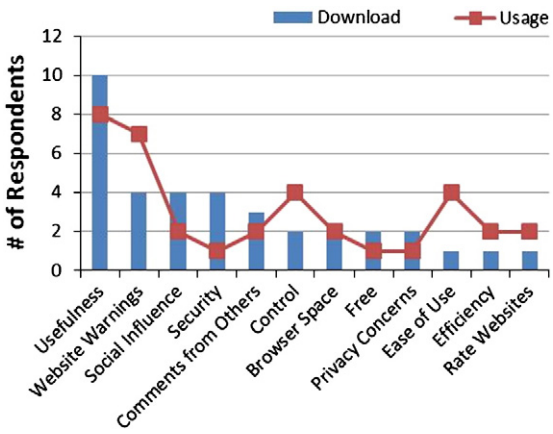

Fig. 7. Technical evaluation: novice.

As discussed previously, the design of the PESS has proven to meet the design principles set out at the beginning of the process. The experts and novices who evaluated the tools agreed that the design principles were met. The experts suggested that certain factors should be considered in the future design of PETs. While we intend to include some of these features in future design efforts, novices indicated that the design as presented would be useful and they would use it.

In summary, the PESS tools provide privacy control tools over two types of user information, far beyond website cookie management:

- Type (A) information provided by users to a website (e.g., address, phone number, and credit card information), and
- Type (B) user data generated during website browsing and usage (e.g., browsing history, uncompleted shopping cart items, digital subscriptions, and transaction history).

An example using the Amazon.com website would work as follows: Registered users could save their Type A information at Amazon.com including users' address, phone number, and optional credit card information. Amazon.com also generates and stores users' Type B information, and allows registered users to browse their Type B information such as recent history of catalog browsing and item searching on Amazon, recent uncompleted shopping cart items, their digital subscriptions, and their recent transaction history. Built on the application-layer making use of web server-end mechanisms (APIs) and pre-defined client–server protocols, the PEControl tool can retrieve users' Type A and Type B information from servers. Built as a browser add-on, the user interface of PEControl allows users to view their Type A and Type B information quickly at the browser, saving users' efforts in visiting a website to find and view their information.

More than just an information-browsing tool, PEControl is also able to deliver users' privacy control settings to individual websites. For example, if Amazon.com allows users to control the number of uncompleted shopping carts to be saved on the server, users can either go to the Amazon.com site to change the setting or directly use the PEControl browser add-on to change the setting. Going to individual websites to change privacy settings might impose cognitive load on users because of the differences of user interfaces and browsing paths among different websites. PEControl provides a consistent and convenient user interface to change privacy control settings for individual websites. PEControl communicates with individual websites in a pre-defined protocol and implements the privacy control via web service and API calls. The technical discussion of these techniques is out of the scope of this paper.

The PESS tool has proven useful in this research. However, it is possible that its widespread acceptance could be problematic since the underlying premise of these solutions is predicated upon users' awareness of online privacy risks and their own privacy needs.[5] Anecdotal evidence suggests that the most effective way to protect online privacy is to combine education and training with the use of technology tools to promote the users' awareness. End-user awareness and training is an especially challenging area in that users vary widely in level of motivations, perceptions of threat severity, and computer self-efficacy [46,50]. Therefore, future research should investigate how to integrate user awareness and training with the design and deployment of privacy-enhancing technologies.

One limitation of our study relates to the fact that for web users, reading reviews may overload them and thus may decrease their website usage. There are a number of well-established techniques developed to address this problem, such as automatic text analysis to extract key points of a text review, and automatic numerical rating and scoring systems based on text reviews. Future research could include these techniques to decrease the overall effort that users have to put with respect to review reading. Integrating a methodological way of handling review information into a tool such as PESS would provide even more information at the hands of users to make wise privacy decisions.

5. Conclusion

Building on the principles of Value Sensitive Design, we have discussed the conceptual and technical investigations of end-user privacy-enhancing tools. Based on the psychological control agency theory, we designed PESS with three privacy-enhancing tools including the search tool for privacy promise and practice (*PESearch*), the privacy control tool for controlling users' personal data (*PEControl*), and the review tool for sharing the ratings and reviews on websites' privacy practices (*PEReview*). We discussed the design values of these privacy-enhancing tools and proposed a prototype system named PESS to integrate these tools. In future work, we expect to extend these investigations, implement and deploy the prototype, and iterate on empirical investigations as well. Overall, the integrated design of privacy-enhancing tools identified in this study will provide a rich understanding of the e-business applications that create personal vulnerabilities, and therefore, inform privacy research in the IS discipline. Our goal is to create an integrative privacy-enhancing solution that, when completed, will empower users with personal control, proxy control, and collective control over their personal information.

[5] We thank an anonymous reviewer for this insight.

Acknowledgments

The authors are very grateful to the anonymous reviewers for their constructive comments, and to Hao Wang for his input and assistance on technical design issues of PESS. The authors also thank Pan Shi for her assistance on the literature review.

References

[1] G. Aggarwal, E. Bursztein, C. Jackson, D. Boneh, An Analysis of Private Browsing Modes in Modern Browsers, In: Proceedings of19th USENIX Security Symposium, Washington, DC, USA, 2010, pp. 79–94.
[2] G. Alonso, H. Kuno, F. Casati, V. Machiraju, Web Services: Concepts, Architectures and Applications, Springer, New York, 2003.
[3] A.I. Antón, J.B. Earp, D. Bolchini, Q. He, C. Jensen, W. Stufflebeam, The lack of clarity in financial privacy policies and the need for standardization, IEEE Security & Privacy 2 (2) (2004) 36–45.
[4] A. Bandura, Self-efficacy mechanism in human agency, American Psychologist 37 (1982) 122–147.
[5] F. Bélanger, R.E. Crossler, Privacy in the digital age: a review of information privacy research in information systems, MIS Quarterly 35 (4) (2011) 1017–1041.
[6] F. Bélanger, J. Hiller, W.J. Smith, Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, The Journal of Strategic Information Systems 11 (3/4) (2002) 245–270.
[7] S. Byers, L. Cranor, D. Kormann, P. McDaniel, Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine, In: The 2004 Workshop on Privacy Enhancing Technologies (PET2004), (Toronto, Canada), 2004, pp. 314–328.
[8] S. Byers, L.F. Cranor, D. Kormann, P. McDaniel, Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine, In: Proceedings of the 4th International Conference on Privacy Enhancing Technologies, Springer-Verlag, Toronto, Canada, 2005, pp. 314–328.
[9] S. Chakrabarti, Mining the Web, Morgan Kaufmann, San Fransisco, CA, 2003.
[10] L.F. Cranor, Web Privacy with P3P, O'Reilly & Associates, Sebastopol, CA, 2002.
[11] L.F. Cranor, S. Byers, D. Kormann, An Analysis of P3P Deployment on Commercial, Government, and Children's Web Sites as of May 2003, In: Technical Report prepared for the 14 May 2003 Federal Trade Commission Workshop on Technologies for Protecting Personal Information, AT&T Labs-Research, Florham Park, NJ, 2003.
[12] M.J. Culnan, 'How Did They Get My Name'? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use, MIS Quarterly 17 (3) (1993) 341–364.
[13] M.J. Culnan, J.R. Bies, Consumer privacy: balancing economic and justice considerations, Journal of Social Issues 59 (2) (2003) 323–342.
[14] A. Czeskis, I. Dermendjieva, H. Yapit, A. Borning, B. Friedman, B. Gill, T. Kohno, Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety, In: Proceedings of the Sixth Symposium on Usable Privacy and Security Redmond, WA, 2010, pp. 1–15.
[15] T. Dinev, P. Hart, Internet privacy concerns and their antecedents — measurement validity and a regression model, Behavior and Information Technology 23 (6) (2004) 413–423.
[16] S. Egelman, L.F. Cranor, J. Hong, You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings, In: Proceedings of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems (CHI'08), 2008, pp. 1065–1074.
[17] EPIC, Pretty Poor Privacy: An Assessment of P3P and Internet Privacy, In: Electronic Privacy Information Center, 2000, http://www.epic.org/reports/prettypoorprivacy.html.
[18] B. Friedman, Value Sensitive Design, In: Encyclopedia of Human-Computer Interaction, Berkshire Publishing Group, Great Barrington, MA, 2004, pp. 769–774.
[19] B. Friedman, P.H. Kahn Jr., A. Borning, Value Sensitive Design and Information Systems, In: P. Zhang, D. Galletta (Eds.), Human–Computer Interaction and Management Information Systems: Foundations, M E Sharpe, Armonk, NY, 2006.
[20] FTC, Protecting Consumer Privacy in an Era of Rapid Change, Federal Trade Commission, 2010.
[21] A. Genkina, L.J. Camp, Re-Embedding Existing Social Networks into Online Experiences to Aid in Trust Assessment, 2005. Available at SSRN: http://ssrn.com/abstract=707139.
[22] A.R. Hevner, S.T. March, J. Park, S. Ram, Design science in information systems research, MIS Quarterly 28 (1) (2004) 75.
[23] J.I. Hong, An Architecture for Privacy-Sensitive Ubiquitous Computing, in: Computer Science Division, University of California at Berkeley, Berkeley, 2005.
[24] X. Hu, G. Wu, Y. Wu, H. Zhang, The effects of web assurance seals on consumers' initial trust in an online vendor: a functional perspective, Decision Support Systems 48 (2) (2010) 407–418.
[25] C. Jensen, C. Potts, Privacy Policies Examined: Fair Warning or Fair Game? GVU Technical Report 03–04, The Georgia Institute of Technology, 2003.
[26] C. Jensen, C. Potts, Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices, In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2004, pp. 471–478.
[27] G. Karjoth, Access control with IBM Tivoli access manager, ACM Transactions on Information and System Security 6 (2) (2003) 232–257.
[28] G. Karjoth, M. Schunter, M. Waidner, The Platform for Enterprise Privacy Practices - Privacy-Enabled Management of Customer Data, In: The 2nd Workshop on Privacy Enhancing Technologies (PET 2002), San Francisco, CA, 2002, pp. 69–84.
[29] O. Kwon, A pervasive P3P-based negotiation mechanism for privacy-aware pervasive e-commerce, Decision Support Systems 50 (1) (2010) 213–221.
[30] R. LaRose, N. Rifon, Your privacy is assured—of being disturbed: comparing web sites with and without privacy seals, New Media and Society 8 (6) (2006) 1009–1029.
[31] R.M. Lee, Doing Research on Sensitive Topics, Sage, 1993.
[32] H. Li, R. Sarathy, H. Xu, The role of affect and cognition on online consumers' willingness to disclose personal information, Decision Support Systems 51 (3) (2011) 434–445.
[33] H. Liang, Y. Xue, Avoidance of information technology threats: a theoretical perspective, MIS Quarterly 33 (1) (2009) 71–90.
[34] W.E. Mackay, Triggers and Barriers to Customizing Software, In: The ACM CHI'91 Human Factors in Computing Systems, New Orleans, LA, 1991, pp. 153–160.
[35] M. Madden, S. Fox, A. Smith, J. Vitak, Digital Footprints: Online Identity Management and Search in the Age of Transparency, Pew Internet & American Life Project, 2008.
[36] K.N. Malhotra, S.S. Kim, J. Agarwal, Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model, Information Systems Research 15 (4) (2004) 336–355.
[37] S.T. March, G.F. Smith, Design and natural science research on information technology, Decision Support Systems 15 (4) (1995) 251–266.
[38] Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9, 2010.
[39] Microsoft, Tracking Protection List, 2011.
[40] Microsoft, How to Manage Cookies in Internet Explorer 9, 2012.
[41] M.B. Miles, A.M. Huberman, Qualitative Data Analysis: An Expanded Sourcebook, Sage Publications, Thousand Oaks, CA, 1994.
[42] J.K. Miller, B. Friedman, G. Jancke, Value Tensions in Design: The Value Sensitive Design, Development, and Appropriation of a Corporation's Groupware System, In: Proceedings of the International ACM Conference on Supporting Group Work, Sanibel Island, Florida, 2007, pp. 281–290.
[43] L.I. Millett, B. Friedman, E. Felten, Cookies and Web Browser Design: Toward Realizing Informed Consent Online, In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Seattle, WA, 2001, pp. 46–52.
[44] G.R. Milne, M.J. Culnan, Strategies for reducing online privacy risks: why consumers read(or don't read) online privacy notices, Journal of Interactive Marketing 18 (3) (2004) 15–29.
[45] A. Miyazaki, S. Krishnamurthy, Internet seals of approval: effects on online privacy policies and consumer perceptions, Journal of Consumer Affairs 36 (1) (2002) 28–49.
[46] S. Pahnila, M. Siponen, A. Mahmood, Employees' Behavior towards IS Security Policy Compliance, In: Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE Computer Society, Big Island, HI, United States, 2007.
[47] PrivacyChoice, PrivacyChoice Tracking Protection List, 2010.
[48] R.W. Proctor, M.A. Ali, K.P.L. Vu, Examining usability of web privacy policies, International Journal of Human Computer Interaction 24 (3) (2006) 307–328.
[49] J. Reagle, L.F. Cranor, The platform for privacy preferences, Association for Computing Machinery, Communications of the ACM 42 (2) (1999) 48.
[50] H.-S. Rhee, Y.U. Ryu, C.-T. Kim, I am fine but you are not: Optimistic bias and illusion of control on information security, In: International Conference on Information Systems, Las Vegas, NV, 2005.
[51] N.J. Rifon, R. LaRose, S.M. Choi, Your privacy is sealed: effects of web privacy seals on trust and personal disclosures, Journal of Consumer Affairs 39 (2) (2005) 339–362.
[52] S. Romanosky, A. Acquisti, J. Hong, L.F. Cranor, B. Friedman, Privacy Patterns for Online Interactions, In: Proceedings of the 2006 Conference on Pattern Languages of Programs, 2006.
[53] S. Sheng, B. Wardman, G. Warner, L.F. Cranor, J. Hong, C. Zhang, An Empirical Analysis of Phishing Blacklists, In: Sixth Conference on Email and Anti-Spam, 2009.
[54] J. Sobey, R. Biddle, P.C. Oorschot, A.S. Patrick, Exploring User Reactions to New Browser Cues for Extended Validation Certificates, In: Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, Málaga, Spain, 2008, pp. 411–427.
[55] G. Staikos, Web Browser Developers Work Together on Security, 2005.
[56] C. Steinfield, H. Bouwman, T. Adelaar, The dynamics of click-and-motor electronic commerce: opportunities and management strategies, International Journal of Electronic Commerce 7 (1) (2002) 93–119.
[57] E.F. Stone, G.H. Gueutal, D.G. Gardner, S. McClure, A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations, Journal of Applied Psychology 68 (3) (1983) 459–468.
[58] Z. Tang, Y.J. Hu, M.D. Smith, Gaining trust through online privacy protection: self-regulation, mandatory standards, or caveat emptor, Journal of Management Information Systems 24 (4) (2008) 153–173.
[59] Truste, Truste Easy Tracking Protection List, 2010.
[60] C.E. Turner, S. Dasgupta, Privacy on the web: an examination of user concerns, technology, and implications for business organizations and individuals, Information Systems Management (2003) 8–18 [Winter].
[61] W3C, Web Service Definition Language (WSDL), The World Wide Web Consortium, 2001.
[62] W3Schools, Browser Statistics, 2011.
[63] T. Whalen, K.M. Inkpen, Gathering Evidence: Use of Visual Security Cues in Web Browsers, In: Proceedings of Graphics Interface 2005, Canadian Human-Computer Communications Society, Victoria, British Columbia, 2005, pp. 137–144.
[64] M. Wu, R.C. Miller, S.L. Garfinkel, Do Security Toolbars Actually Prevent Phishing Attacks? In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montréal, Québec, Canada, 2006, pp. 601–610.

[65] H. Xu, H.H. Teo, Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective, In: Proceedings of the Twenty-Fifth Annual International Conference on Information Systems (ICIS 2004), Washington, D. C., United States, 2004, pp. 793–806.
[66] H. Xu, N. Irani, S. Zhu, W. Xu, Alleviating Parental Concerns for Children's Online Privacy: A Value Sensitive Design Investigation, Proceedings, ICIS, 2008.
[67] H. Xu, T. Dinev, H.J. Smith, P. Hart, Information privacy concerns: linking individual perceptions with institutional privacy assurances, Journal of the Association for Information Systems 12 (12) (2011) 798–824.
[68] H. Xu, X. Luo, J.M. Carroll, M.B. Rosson, The personalization privacy paradox: a study of privacy decision making process for location-awareness marketing, Decision Support Systems 51 (1) (2011) 42–52.
[69] S. Yamaguchi, Culture and Control Orientations, In: D. Matsumoto (Ed.), The Handbook of Culture and Psychology, Oxford University Press, New York, 2001, pp. 223–243.
[70] N. Zhang, W. Zhao, Privacy-Preserving OLAP: An Information-Theoretic Approach, IEEE Transactions on Knowledge and Data Engineering (TKDE) 23 (1) (2011) 122–138.

Heng Xu is an Associate Professor of Information Sciences and Technology at The Pennsylvania State University where she is a recipient of the endowed PNC Technologies Career Development Professorship. She has conducted research in the areas of information privacy and security, human-computer interaction, and technological innovation adoption. Her current research focus is on the interplay between social and technological issues associated with information privacy and security. Her research projects have been dealing with the conceptualization, intervention, and design aspects of privacy and security. Her work has appeared in *Decision Support Systems*, *Information & Management*, *Information Systems Research*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *MIS Quarterly*, and in other journals. She serves on the editorial review board for *IEEE Transactions on Engineering Management*, *Information Systems Journal*, *Internet Research*, and other journals. In 2010, she was a recipient of the Faculty Early Career Development (CAREER) Award by the National Science Foundation.

Robert E. Crossler is an Assistant Professor in the Management and Information Systems department at Mississippi State University. His research focuses on the factors that affect the security and privacy decisions that individuals make. He has several publications in the IS field, including such outlets as MIS Quarterly, Journal of Information Systems Security, Americas Conference on Information Systems, The Annual Conference of the Decision Sciences Institute, Hawaii International Conference on System Sciences, and many others. He also serves on the editorial review board for Information Resources Management Journal and Journal of Information Systems Security and has served as Associate Editor for the International Conference on Information Systems and the European Conference on Information Systems.

France Bélanger is Tom & Daisy Byrd Senior Faculty Fellow and Professor in the department of Accounting and Information Systems at Virginia Tech. Her research focuses on the use of communication technologies, in particular for technology mediated work and e-business, and on information privacy and security. Her award winning work has been published in leading IS journals, including Information Systems Research, MIS Quarterly, Journal of the Association for Information Systems, Journal of Strategic Information Systems, Information Systems Journal, various IEEE Transactions, and many others. Dr. Bélanger co-authored three books. She is or has been Guest Senior Editor and Associate Editor for MIS Quarterly, Associate Editor for Information Systems Research, and other journals. Her work has been funded by several agencies, corporations and research centers, including the National Science Foundation. She was named Fulbright Distinguished Chair in 2006 (Portugal) and Erskine Visiting Fellow in 2009 (New Zealand).