Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2008 Proceedings

International Conference on Information Systems (ICIS)

2008

Alleviating Parental Concerns for Children's Online Privacy: A Value Sensitive Design Investigation

Heng Xu
Pennsylvania State University, hxu@ist.psu.edu

Nazneen Irani
Pennsylvania State University, nni100@psu.edu

Sencun Zhu
Pennsylvania State University, szhu@cse.psu.edu

Wei Xu
Pennsylvania State University, wxx104@psu.edu

Recommended Citation

Xu, Heng; Irani, Nazneen; Zhu, Sencun; and Xu, Wei, "Alleviating Parental Concerns for Children's Online Privacy: A Value Sensitive Design Investigation" (2008). *ICIS 2008 Proceedings*. 106.
http://aisel.aisnet.org/icis2008/106

ALLEVIATING PARENTAL CONCERNS FOR CHILDREN'S ONLINE PRIVACY: A VALUE SENSITIVE DESIGN INVESTIGATION

Rassurer les parents sur le respect de la vie privée de leurs enfants : une étude de conception prenant en considération les valeurs éthiques

Research-in-Progress

Heng Xu
Pennsylvania State University
University Park, PA 16802
hxu@ist.psu.edu

Nazneen Irani
Pennsylvania State University
University Park, PA 16802
nni100@psu.edu

Sencun Zhu
Pennsylvania State University
University Park, PA 16802
szhu@cse.psu.edu

Wei Xu
Pennsylvania State University
University Park, PA 16802
wxx104@psu.edu

Abstract

The objective of this research is to address the acute privacy challenge of protecting children's online safety by proposing a technological solution to empower parental control over their child's personal information disclosed online. As a preliminary conceptual investigation, this paper draws on the social, psychological, and legal perspectives of privacy to derive three design principles. We propose that, the technical systems for protecting children's online privacy (a) should protect children's personal information online while enabling their access to appropriate online content, (b) should maximally facilitate parental involvement of their children's online activities, and (c) should comply with legal requirements in terms of notice, choice, access and security. This study reported here is novel to the extent that existing IS research has not systematically examined the privacy issues from the VSD perspective. We believe that, using the groundwork laid down in this study, future research along these directions could contribute significantly to addressing parental concerns for children's online safety.

Keywords: Children's online privacy, value sensitive design (VSD), privacy law, privacy enhancing technologies.

Résumé

L'objectif de cette recherche est d'aborder le défi du respect de la vie privée et de la sécurité des enfants sur internet en proposant une solution technologique pour renforcer le contrôle parental sur les renseignements personnels de leurs enfants qui sont disponibles en ligne. Dans une étude conceptuelle préliminaire, ce papier s'appuie sur les perspectives sociale, psychologique et juridique de la vie privée pour de tirer trois principes de conception.

1 Introduction

The number of children accessing the internet is constantly on the rise and protecting their privacy is becoming a major challenge. By nature, children's ability to thinking critically is limited due the stage of their cognitive skills developmentally, and they are more naïve in their decisions. For instance, nearly half of teens (47%) are not worried about others using their personal information on the Internet (WWK 2007). Operators online exploit this factor by luring children to attractive prizes, games, gifts and offers in exchange of their personal information or their parents' information. Unsurprisingly, parents and advocates voice great concerns regarding the privacy loss of children because of the interactive features of online marketing (Youn 2005). Furthermore, Internet is even to be blamed for the rise in child porn as the offenders have the resources to remain anonymous online while children reveal their information (BBC 2004).

In the context of information privacy protection, Fair Information Practice (FIP) principles have served as a set of global principles which guide privacy regulation and industry practices (FTC 2000). FIP principles are a set of normative standards including the stipulations that individuals be given: *notice* that their personal information is being collected, *choice* with regard to use of their information, *access* to personal data records, and *security* for these data records (FTC 2000). Particularly, FIP principles are global standards for the ethical use of personal information and are at the heart of US industry guidelines and privacy laws, and European Union privacy directives (Culnan and Armstrong 1999).

To address the acute challenge of protecting children's online privacy, in 1998, the U.S. Congress enacted the Children's Online Privacy Protection Act (COPPA) to implement the FIP principles. COPPA applies to any operator of a website or online service that is directed to collect personal information from a child under the age of 13. Unfortunately, the enforcement of FIP principles through the COPPA has not been effective enough, which has resulted in web operators getting civil penalties due to violating the FIP principles. The largest penalty that the FTC has ever obtained in a COPPA case was the social networking website, Xanga.com which violated the *notice* principle by collecting personal information from children under the age of 13 without first notifying parents and obtaining their consent (FTC 2006). The company has been ordered to pay $1 million in a settlement with the Federal Trade Commission (FTC) for violating the COPPA (FTC 2006). A more recent case was filed against Imbee.com which enabled more than 10,500 children to create accounts by submitting their first and last names, dates of birth, personal e-mail addresses, gender, user-names and passwords prior to the site's providing *notice* to parents or obtaining their consent (FTC 2008).

Those COPPA violation cases raise challenges for the FIP enforcement: making sure that all websites abide by the rule is a difficult task which cannot be achieved by relying on website operators alone. Protecting children's innocence and at the same time protecting their privacy remains a huge social-technical challenge (FTC 2007). The objective of this research, therefore, is to address such challenge by discussing children's online privacy as a social, technical, and policy issue; outlining the technical and social dimensions of protecting children's online safety without overly constraining their freedom to engage in appropriate online activities; and justifying the need for a common understanding for designing for children's online privacy.

In what follows, we first introduce the theoretical and methodological framework for our research, describing Value Sensitive Design (VSD) method that derives our design principles. Then we present the state of the art by discussing existing solutions for addressing online privacy in general and for addressing particular concerns pertaining to children's online privacy. This is followed by a brief discussion of our research plan for the technical investigation and empirical evaluation. We close by arguing that the VSD framework offers unique promise for addressing children's online privacy.

2 Privacy as a Design Value

Value sensitive design (VSD) is an approach to the design of information and computer systems that accounts for human values in a principled and comprehensive manner throughout the design process (Friedman 2004; Friedman et al. 2006). It is particularly useful for our research because such method emphasizes values with moral import such as privacy and trust (Friedman 2004; Friedman et al. 2006). This design method embeds explicit values choices, documents those choices, and thus enables adoption and alteration of technologies to be informed choices for the appropriate social context (Camp and Connelly 2007).

As Camp et al. (2007) pointed out, the sheer complexity of understanding a value as amorphous as privacy has been a challenge in applying VSD. In fact, the difficulty in defining common ground of privacy will likely become more pronounced in the next few years. According to a 2007 study sponsored by the National Research Council (NRC 2007), the relationship between information privacy and society is now under pressure due to several factors that are "changing and expanding in scale with unprecedented speed in terms of our ability to understand and contend with their implications to our world, in general, and our privacy, in particular." Factors related to technological change (e.g., data collection, communications), to societal trends (e.g., globalization, cross-border data flow, increases in social networking) are combining to force a reconsideration of basic privacy concepts and their implications (NRC 2007). Thus rather than drawing on a monolithic concept of privacy from a single discipline, we try to leverage diverse paradigms to understand design values of privacy.

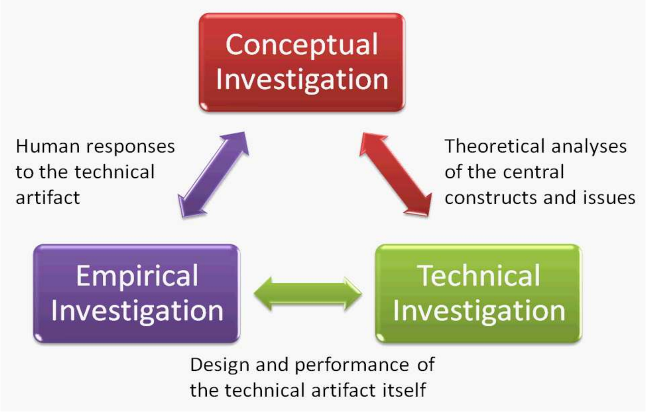
Conceptual Investigation
Human responses to the technical artifact
Theoretical analyses of the central constructs and issues
Empirical Investigation
Technical Investigation
Design and performance of the technical artifact itself

Figure 1. Value Sensitive Design (VSD) Method

As shown in Figure 1, VSD adopts a tripartite methodology by systematically integrating and iterating on three types of investigations (Friedman 2004; Friedman et al. 2006): *conceptual investigations* comprise philosophically informed analyses of the central constructs and issues under investigation; *technical investigations* focus on the design and performance of the technology itself; *empirical investigations* focus on the human responses to the technical artifact. In this paper, we offer our initial start at a conceptual investigation based on three main perspectives from which the notions of privacy are commonly described and analyzed (see Table 1).

Table 1. Three Paradigms regarding the Concept of Privacy (Adapted from Patil and Kobsa (2008))

Paradigms	Theoretical Lenses	Driven Force	Consequences of Privacy Violation
Contextual Nature of Privacy	Social	Individuals' own experiences and social expectations	Potential embarrassment or breakdown in relationship(s) etc.
Privacy as Control	Psychological	Autonomy, self-efficacy and trust	Concern/worry about data misuse and identity theft
Legal Protections	Normative	National or supra-national legislative act	Civil and/or criminal penalties

2.1 Contextual Nature of Privacy

One very important perspective considers the contextual nature of privacy (Nissenbaum 2004). In more recent privacy literature, such contextual paradigm of privacy recognizes that privacy both influences and can be influenced by various situational and societal forces. Individuals' desire for privacy is innately dynamic (Sheehan 2002), and influenced by various situational forces, such as pressures from others, societal norms, and processes of surveillance used to enforce them (Nissenbaum 2004). Altman (1975) conceptualized privacy decision-making as a dialectic and dynamic boundary regulation process. As a *dialectic* process, privacy is "conditioned by individuals' own experiences and social expectations, and by those of others with whom they interact" (Palen and Dourish 2003, p.129). As a *dynamic* process, privacy is "understood to be under continuous negotiation and management", with the *boundary* that distinguishes privacy and publicity defined according to circumstance (Palen and Dourish 2003, p.129).

Protecting children's privacy is complicated by the fact that children's privacy is a socially constructed value that reflects the child-parent relationship – that of protecting children's online privacy without overly constraining their freedom to engage in appropriate online activities. For instance, according to COPPA, the website operator must obtain verifiable parental consent before personal information is collected from a child. Unfortunately, obtaining parental consent is more socially complicated in this context. Because websites are far away from the parents, how is the site operator going to ensure that the person vouching for the child's age is really the parent or even an adult? According to a recent FTC report, it is concluded that age verification technologies have not kept pace with other developments [5]. Another social complexity associated with children's privacy is that, children quickly learned that if they say they are below thirteen they will be prohibited from using many sites. As a result, children regularly lie about their age online. Seeing these social complexities in the context of protecting children's privacy, we propose following design principle for protecting children's online privacy:

Design Principle #1: The technical systems for protecting children's online privacy should make a balance between protecting children's personal information online and preserving their ability to access appropriate content.

2.2 Privacy as Control

A second major paradigm considers privacy in terms of *control* of personal information. This perspective is found in various prior works (e.g., Altman 1977; Johnson 1974; Laufer et al. 1973; Margulis 1974; Westin 1967) which have contributed to and stimulated the paradigm of privacy as a control related concept. A number of privacy theorists have put emphases on the concept of control when defining privacy (e.g., Margulis 1977; Margulis 2003; Proshansky et al. 1970; Stone et al. 1983; Westin 1967). For example, Wolfe and Laufer (1974) suggested that "the need and ability to exert control over self, objects, spaces, information and behavior is a critical element in any concept of privacy" (p.3). Empirical evidence revealed that control is one of the key factors which provide the greatest degree of explanation for privacy concern (Dinev and Hart 2004; Goodwin 1991; Nowak and Phelps 1997; Phelps et al. 2000; Sheehan and Hoy 2000). Individuals perceive less privacy concerns when they believe that they will be able to control the use of the information (Culnan and Armstrong 1999).

Based on control agency theory (Yamaguchi 2001), two types of control have been identified by Xu (2007) in the privacy context: 1) *personal control* in which the self acts as the control agent, 2) *proxy control* in which external entities act as the control agent. End-user privacy-protecting tools such as cookie managers allow users to protect their information privacy by directly controlling the flow of their own personal information to others (Burkert 1997). As is evident, with end-user privacy protecting tools, the agent of control is the *self*; and the effects of this mechanism arise due to the opportunity for direct personal control. With regard to proxy control, trusted third party (TTP) is a commonly used approach that mainly consists of an entity facilitating interactions between users and websites who both trust the third party to secure their interactions. TTP solution to privacy is one example of proxy control that is created to provide third-party assurances to users based on a voluntary contractual relationship between websites and the third party. On behalf of users, the TTP acts as the control agent for users to exercise proxy control over the flow of personal information.

This paradigm of privacy as control brings rise to the debate among scholars and practitioners on the effectiveness of these two (and other) mechanisms for privacy control: Whose responsibility of protecting children's privacy – parents themselves or websites or TTPs? Which control approach will be more effective, personal control or proxy control? Cognitively, self agency (through which personal control is exercised) should motivate greater user engagement and involvement, which is likely to result in positive attitudes given its guaranteed consonance with individual interests (Skinner et al. 1988; Yamaguchi 2001). Drawing on recent privacy literature on comparing the relative effectiveness of personal vs. proxy privacy control approaches (Edelman 2006; Xu and Teo 2004), we propose that the technical systems for protecting children's online privacy should maximally empower parental control over children's personal information online. This is also consistent with the conclusion from two blue-ribbon panels conducted by the U.S. Congress, which suggested that that one of the most effective ways is to facilitate parental involvement by letting parents decide what information their children could disclose, and what content their children should access (CDT 2008; Thierer 2007). Therefore, we propose following design principle for protecting children's online privacy:

Design Principle #2: The technical systems for protecting children's online privacy should maximally facilitate parental involvement of their children's online activities.

2.3 Legal Expectations on Protecting Children's Online Privacy

Government legislation is another commonly used approach that relies on the judicial and legislative branches of a government for protecting personal information (Swire 1997). Legislative efforts to implement FIP principles could specifically address concerns regarding fairness and accountability for privacy protection actions, thereby providing individuals with a sense of security (Zucker 1986). In the context of protecting children's online privacy, COPPA was enacted in the U.S. to: (1) enhance parental involvement in their children's online activities in order to protect children's privacy in the online environment; (2) protect the safety of children at places in the online environment such as chat rooms, home pages, email accounts, and bulletin boards in which children may make public postings of identifying information; (3) maintain the security of children's personal information collected online; and (4) limit the collection of personal information from children without parental consent.

In the U.S., in terms of implementing FIP principles, COPPA addressed *notice* and *choice* by requiring that, before personal information is collected from a child, a parent must: receive notice of the operator's personal information collection, use, and disclosure practices; and authorize any collection, use, and/or disclosure of the personal information. *Access* requires that the parent of any child who has provided personal information to an operator has the right to request access to such information. *Security* requires that an operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. In an environment where privacy law on protecting children's privacy exists, any technical solution should comply with the legal requirements. Therefore, we propose following design principle:

Design Principle #3: The technical systems for protecting children's online privacy should comply with legal requirements in terms of notice, choice, access and security.

3 State of the Art

Below we discuss existing solutions for addressing online privacy in general and then the efforts which have been targeted at protecting children's privacy.

3.1 General Solutions

Cookies, a unique identifier that a web server places on user's computer that can be used to retrieve their records from the databases, authenticate, identify and track users, were seen as a major threat to user's online privacy. Third party cookies could be linked to user's collected browsing history which makes them a greater threat. COPPA recognizes cookies to be a privacy threat and disallows operators from collecting cookie that can be linked to a child. As a solution, most web browsers provide cookie control and blocking features to give users the option of protecting their privacy. Cookie blocking software is effective but addresses a very small part of the requirements of COPPA. These cookie-related solutions do not contribute to the scenarios where websites explicitly collect personally identifiable information from children under the age of 13.

The anonymizer (Bauer October 2003; Dingledine et al. 2004; Pinto et al. 2004) is another solution that protects user's privacy by providing a way for anonymous web browsing. All communication is directed through an intermediary proxy server to hide the true origination of a message. Thus cookies cannot be placed on the user's browser and the user's true IP address cannot be tracked. The anonymizer serves as a good privacy solution to protect online privacy in general but it is not sufficient for protecting children's online safety. For example, anonymous browsing is contradictory in the context of protecting children's online privacy because we need the website operator to recognize the client as a child and take additional precautionary steps to protect their online privacy. In addition, anonymous browsing may encourage children to access objectionable material once they are aware that they are not being identified as children.

The Platform for Privacy Preferences Project (P3P) is a protocol designed to provide a way for a Web site to encode its human readable privacy practices in a machine-readable format known as a P3P policy (Cranor 2002). Users could employ a P3P user agent (e.g., AT&T Privacy Bird) to evaluate whether an online company implements P3P-compliant privacy policy by configuring their privacy preferences using a series of checkboxes (Cranor 2002). While P3P and its user agents provides users with the privacy options of notice (i.e., notifying users whether a Web site's privacy policy conflicts with their privacy preferences) and choice (i.e., allowing users to make sound decisions on whether to provide personal information based on the user agent's notice), P3P lacks the *enforcement* mechanism to ensure sites act according to their privacy policies. Hence, it has been suggested that the use of P3P in the absence of risk assurance mechanisms shifts the onus primarily onto the individual user to protect herself (Xu et al. 2005). Recent studies (Egelman and Cranor 2006; Reay et al. 2007) have shown that few websites adopt P3P, which limits P3P's impact as a privacy enhancing approach. In addition, P3P has not specifically addressed parental concerns for children's online privacy.

Another popular approach to privacy assurance is through self-regulatory efforts which involve the setting of standards either by the website itself or an industry group and the voluntary adherence to the set standards or policies (Culnan and Bies 2003). Under a self-regulatory approach to regulating children's online privacy, groups like TRUSTe have been active as the third party entities policing children's privacy and promoting trustworthiness to websites through seals of approval. By becoming a member of these private watchdog groups, a website is permitted to post the seal of approval. These seal programs provide a means to guarantee that members abide by a set of clearly identified self-regulatory policies (Culnan and Bies 2003). However, research has shown that, most privacy policies posted online are written in jargon and ambiguous language and thus readability is low (Crossler et al. 2007b; Culnan and Milne 2001; Milne and Culnan 2004). For those parents who are not technically sound or are unaware of COPPA, they usually fail to make informed decisions for their child's information disclosure. In addition, it has been found that few parents recognize privacy seals (Crossler et al. 2007b). Thus, we conclude that the self-regulatory approach to children's privacy through privacy policies or privacy seals cannot be adopted as stand-alone solutions but as an additional protection layer complimentary to technical enforcement of COPPA.

3.2 Solutions Targeted at Children's Online Safety

Many software control packages have been introduced to empower parental control of children's online behavior. Microsoft has introduced parental controls built into Windows Vista, designed to help parents manage what their children can do on computers. Apart from OS features, there also exist dedicated software packages such as Net Nanny and browser extensions such as the Parental Control toolbar. Solutions targeted toward children's online safety are mostly variations of blocking software and content filters. These software packages usually block outbound information from client and prevent children from revealing sensitive information, without supporting the function of obtaining verifiable parental consent. However, completely blocking information that a child submits to websites during registration may prevent the child from gaining access to a service. Recently, a call for protecting children's personal information online while enabling their access to appropriate content has been initiated by industry practitioners and government agencies (Thierer 2007). We therefore aim to make such balance in our technical development.

POCKET (Crossler et al. 2007a) provides a tool to enable parents to configure privacy settings for their children and it extends the merchant policy to include data items specified by COPPA and automates the exchange of personal information between the child and server, involving with a Trusted Third Party (TTP). We believe that the design principles of POCKET however have some limitations. First, a server-side solution is not desirable since the threats may be from the operator itself. Second, compromise of a TTP is another factor to be considered since all trust has been vested in the TTP's capabilities to protect the client and a successful attack on the TTP could bring down the entire trust model. TTP requires merchants to abide by the rules set by the TTP, but few, if not no steps, are taken to verify if the website operators conform to the policies agreed upon. This can lead to problems if a website receives the TTP's approval and then carries out malicious activities.

4 Technical Investigation, Future Research, and Conclusion

Following the philosophy of VSD, the conceptual investigations can now be employed to help structure the first iteration of a technical investigation. As discussed earlier, existing solutions to privacy protection appear insufficient to address the social complexities associated with protecting children's online privacy. To address these gaps, we are in the process of developing a tool named as COP (Children's Online Privacy protection tool) to provide technical mechanisms for protecting children's online privacy. Three design principles derived from our conceptual investigations will be applied to structure the first iterations of the COP design. At the ICIS conference, we will be able to demonstrate the prototype of COP together with preliminary user evaluation results.

In future work, we expect to extend these investigations, complete the prototype implementation, and iterate on empirical investigations. Following the philosophy of VSD, empirical investigations will be performed to examine and evaluate human responses to the technical artifact (i.e., COP). Our research design will use complementary strategies for empirical evaluation, integrated with qualitative and quantitative methods. Focus group will first be conducted to explore parents' general privacy attitudes and behavior and to evaluate the COP design. Upon completing the COP prototype implementation, field experiment will be conducted in naturalistic settings by dividing users to two groups, where one will be treated as the control group, and the other group will be provided the opportunity to employ the COP toolkit we develop. We will recruit our experiment participants who have children under 13 from an emailing list containing over 2,000 contacts of working staff at a large university in U.S. Our recruiting messages will explain who we are and what we are trying to do (i.e., the purpose of this study), and invited participation. At the final stage of the experiment, participants will be asked to complete a questionnaire measuring the effectiveness of using the COP.

Overall, the objective of this research is to address the acute privacy challenge of protecting children's online privacy by utilizing the VSD approach that adopts a tripartite methodology by systematically integrating and iterating on conceptual, technical and empirical investigations of privacy. This study reported here is novel to the extent that existing IS research has not systematically examined the privacy issues from the VSD perspective. We believe that, using the groundwork laid down in this study, future research along these directions could contribute significantly to minimizing parental concerns for children's online safety.

5 References

Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Brooks/Cole Publishing, Monterey, CA, 1975.

Altman, I. "Privacy Regulation: Culturally Universal or Culturally Specific?," *Journal of Social Issues* (33:3) 1977, pp 66-84.

Bauer, M. "New Covert Channels in HTTP: Adding UnwittingWeb Browsers to Anonymity Sets," in: *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2003)*, Washington, DC, October 2003.

BBC. Net blamed for rise in child porn. 2004, http://news.bbc.co.uk/1/hi/technology/3387377.stm.

Burkert, H. "Privacy-enhancing technologies: typology, critique, vision," in: *Technology and Privacy: the New Landscape,* P. Agre and M.Rotenberg (eds.), MIT Press, Cambridge, MA, 1997.

Camp, L.J., and Connelly, K. "Privacy in Ubiquitous Computing," in: *Digital Privacy: Theory, Technologies and Practices,* Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis and C. Lambrinoudakis (eds.), Taylor & Frances, New York, NY, 2007.

CDT. Child Safety and Free Speech Issues in the 110 Congress. *Center for Democracy and Technology*. 2008, www.cdt.org/speech/20080206freespeechincongress.pdf

Cranor, L., F. *Web privacy with P3P*, O'Reilly, Sebastopol, CA, 2002.

Crossler, R., Belanger, F., Hiller, J., Aggarwal, P., Channakeshava, K., Bian, K., Park, J., and Hsiao, M. "The Development of a Tool to Protect Children's Privacy Online," in: *Annual Workshop on Information Security and Assurance*, Montréal, Canada, 2007a.

Crossler, R., Belanger, F., Hiller, J., Aggarwal, P., Channakeshava, K., Bian, K., Park, J., and Hsiao, M. "Parents and the Internet: Privacy Awareness, Practices, and Control," in: *Proceedings of Americas' Conference on Information Systems*, KeyStone, Co, 2007b.

Culnan, M.J., and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), Jan-Feb 1999, pp 104-115.

Culnan, M.J., and Bies, J.R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2) 2003, pp 323-342.

Culnan, M.J., and Milne, G.R. "The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses.," in: *Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices*, Washington, D.C., 2001.

Dinev, T., and Hart, P. "Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model," *Behavior and Information Technology* (23:6) 2004, pp 413-423.

Dingledine, R., Mathewson, N., and Syverson, P. "Tor: The second-generation onion router," in: *Proceedings of the 13th USENIX Security Symposium*, 2004.

Edelman, B. "Adverse Selection in Online "Trust" Certifications," Harvard University, 2006.

Egelman, S., and Cranor, L.F. "An Analysis of P3P-Enabled Web Sites among Top-20 Search Results," *Eighth International Conference on Electronic Commerce*, Fredericton, New Brunswick, Canada, 2006.

Friedman, B. "Value Sensitive Design. Encyclopedia of human-computer interaction," Berkshire Publishing Group, Great Barrington, MA, 2004, pp. 769-774.

Friedman, B., Kahn, P.H., Jr., and Borning, A. "Value Sensitive Design and information systems," in: *Human-Computer Interaction and Management Information Systems: Foundations,* P. Zhang and D. Galletta (eds.), M E Sharpe, Armonk, NY, 2006.

FTC. Privacy Online: Fair Information Practices in the Electronic Marketplace *Federal Trade Commission*. 2000, http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

FTC. Xanga.com to pay $1 Million for Violating Children's Online privacy Protection Rule. 2006, http://www.ftc.gov/opa/2006/09/xanga.shtm.

FTC. COPPA Protects Children But Challenges Lie Ahead. 2007, http://www.ftc.gov/opa/2007/02/copparpt.shtm.

FTC. Imbee.com Settles FTC Charges Social Networking Site for Kids Violated the Children’s Online Privacy Protection Act; Settlement Includes $130,000 Civil Penalty. 2008, http://www.ftc.gov/opa/2008/01/imbee.shtm.

Goodwin, C. "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing* (10:1) 1991, pp 149-166.

Johnson, C.A. "Privacy as Personal Control," in: *Man-Environment Interactions: Evaluations and Applications: Part 2,* D.H. Carson (ed.), Environmental Design Research Association, Washington, D.C., 1974, pp. 83-100.

Laufer, R.S., Proshansky, H.M., and Wolfe, M. "Some Analytic Dimensions of Privacy," *Paper presented at the meeting of the Third International Architectural Psychology Conference*, Lund, Sweden, 1973.

Margulis, S.T. "Conceptions of Privacy - Current Status and Next Steps," *Journal of Social Issues* (33:3) 1977, pp 5-21.

Margulis, S.T. "Privacy as a social issue and behavioral concept," *Journal of Social Issues* (59:2) 2003, pp 243-261.

Margulis, T.S. "Privacy as Behavioral Phenomenon: Coming of Age (1)," in: *Man-Environment Interactions: Evaluations and Applications: Part 2,* D.H. Carson (ed.), Environmental Design Research Association, Washington, D.C., 1974, pp. 101-123.

Milne, G.R., and Culnan, M.J. "Strategies for reducing online privacy risks: Why consumers read(or don't read) online privacy notices," *Journal of Interactive Marketing* (18:3) 2004, pp 15-29.

Nissenbaum, H. "Privacy as Contextual Integrity," *Washington Law Review* (79:1) 2004.

Nowak, J.G., and Phelps, J. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters,," *Journal of Direct Marketing* (11:4), Fall 1997, pp 94-108.

NRC *Engaging Privacy and Information Technology in a Digital Age*, National Academies Press, Washington, DC, 2007.

Palen, L., and Dourish, P. "Unpacking "privacy" for a networked world," *Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM Press, Ft. Lauderdale, Fl., 2003, pp. 129-136.

Patil, S., and Kobsa, A. " Privacy Considerations in Awareness Systems: Designing with Privacy in Mind," in: *Awareness Systems: Advances in Theory, Methodology and Design,* P. Markopoulos, B.d. Ruyter and W. Mackay (eds.), Springer Verlag, Berlin, Heidelberg, New York, 2008.

Phelps, J., Nowak, G., and Ferrell, E. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1) 2000, pp 27-41.

Pinto, R., Ishitani, L., Almeida, V., Júnior, M.W., Fonseca, A.F., and Castro, D.F. "Masks: Managing Anonymity while Sharing knowledge to Servers," in: *Proc. of IFIP International Federation for Information Processing*, Springer Boston, 2004, pp. 501-515.

Proshansky, H.M., Ittelson, W.H., and Rivin, L.G. *Environmental Psychology: Man and His Physical Setting*, Holt, Rinehart, and Winston, New York, 1970.

Reay, I., Beatty, P., Dick, S., and Miller, J. "A Survey and Analysis of the P3P Protocol’s Agents, Adoption, Maintenance and Future," *IEEE Transactions on Dependable & Secure Computing* (4:2) 2007, pp 151-164.

Sheehan, K.B. "Toward a typology of Internet users and online privacy concerns," *Information Society* (18:1), Jan-Feb 2002, pp 21-32.

Sheehan, K.B., and Hoy, G.M. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy and Marketing* (19:1) 2000, pp 62-73.

Skinner, E.A., Chapman, M., and Baltes, P.B. "Control, Means-Ends, and Agency Believes: A New Conceptualization and its Measurement During Childhood," *Journal of Personality and Social Psychology* (54) 1988, pp 117-133.

Stone, E.F., Gueutal, G.H., Gardner, D.G., and McClure, S. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology* (68:3) 1983, pp 459-468.

Swire, P.P. "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," in: *Privacy and Self-Regulation in the Information Age,* W.M. Daley and L. Irving (eds.), Department of Commerce, U.S.A., Washington, D.C., 1997, pp. 3-19.

Thierer, A. "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions," *Progress & Freedom Foundation Progress on Point Paper* (14:5) 2007.

Westin, A.F. *Privacy and Freedom*, Atheneum, New York, 1967.

Wolfe, M., and Laufer, R.S. "The Concept of Privacy in Childhood and Adolescence," in: *Privacy as a Behavioral Phenomenon, Symposium Presented at the Meeting of the Environmental Design Research Association,* S.T. Margulis (ed.), Milwaukee, 1974.

WWK. Teen Research Unlimited: Cox Communications Teen Internet safety Survey Wave II. 2007, http://www.webwisekids.org/index.asp?page=statistics.

Xu, H. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," *Proceedings of 28th Annual International Conference on Information Systems (ICIS 2007)*, Montréal, Canada, 2007.

Xu, H., and Teo, H.H. "Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective," *Proceedings of the Twenty-Fifth Annual International Conference on Information Systems (ICIS 2004)*, Washington, D. C., United States, 2004, pp. 793-806.

Xu, H., Teo, H.H., and Tan, B.C.Y. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," *Proceedings of 26th Annual International Conference on Information Systems (ICIS 2005)*, Las Vegas, NV, 2005, pp. 897-910.

Yamaguchi, S. "Culture and Control Orientations," in: *The Handbook of Culture and Psychology,* D. Matsumoto (ed.), Oxford University Press, New York, 2001, pp. 223-243.

Youn, S. "Teenagers'Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach," *Journal of Broadcasting & Electronic Media* (49:1) 2005, pp 86-110.

Zucker, L.G. "Production of trust: Institutional sources of economic structure, 1840-1920," in: *Research in Organizational Behavior,* B.M. Staw and L.L. Cummings (eds.), JAI Press, Greenwich,CT, 1986, pp. 53-111.