Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

12-31-2007

Parents and the Internet: Privacy Awareness, Practices and Control

Michael Hsiao

France Belanger
Virginia Tech

Janine Hiller

Payal Aggarwal

Karthik Channakeshava

See next page for additional authors

Authors
Michael Hsiao, France Belanger, Janine Hiller, Payal Aggarwal, Karthik Channakeshava, Kaigui Bian, Jung-Min Park, and Robert Crossler

PARENTS AND THE INTERNET: PRIVACY AWARENESS, PRACTICES, AND CONTROL

Robert Crossler[1], France Belanger[1], Janine Hiller[2], Payal Aggarwal[2], Karthik Channakeshava[3], Kaigui Bian[3], Jung-Min Park[3], and Michael Hsiao[3]
[1]Accounting and Information Systems, [2]Finance, Insurance and Business, [3]Bradley Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg, VA 24061
(robc, belanger, jhiller, payal, kchannak, kgbian, ,jungmin, hsiao) @vt.edu

Abstract

As children increasingly use the Internet, there have been mounting concerns about their privacy online. As a result, the U.S. Congress enacted the Children's Online Privacy Protection Act (COPPA) to prohibit websites from collecting information from children under 13 years of age without verifiable parental consent. Unfortunately, few technologies are available for parents to provide this consent. Further, few parents are aware of the laws and technologies available. This research explored parental awareness of laws and technologies associated with protecting children's privacy online, and usage of technologies and techniques for parental control, using focus group research. The results of the study are used to propose an emergent framework of factors that will impact use of privacy protection tools and techniques by parents.

Keywords
Privacy, COPPA, Focus Groups, Internet, Children's Privacy

Introduction

A paramount concern of individuals using the Internet is the protection of their children's privacy. As a group, children use the Internet more than any other demographic set in the USA: 65% of children between the ages of 10 and 13 use the Internet (NTIA 2002). Even the simple promise of a small prize can easily convince children to share personal information (Turow 2001). With estimates suggesting that 77 million children will be using the Internet (Kawamoto 2004), and with the escalating threat of insidious child predators and phishing scams in recent years, effective protection of children's privacy in cyberspace is a pressing issue.

In 1996, a Federal Trade Commission (FTC) survey of websites found that 86% of sites collected information from children, yet only 30% had privacy policies, and a mere 4% asked for parental consent to do so. Two years later, the number of websites collecting information from children increased to 89%, while 42% stated a privacy policy; yet less than 11% required some form of parental consent. In reaction to the documented and widespread collection of information from children and related abuses, in 1998 the U.S. Congress enacted the Children's Online Privacy Protection Act (COPPA), which took effect in 2000.

COPPA prohibits websites from collecting information from children under 13 years of age without verifiable parental consent, and requires websites to give parents notice of their information practices and inform them of how they will use collected information. Although originally the FTC stated that its rule regarding parental consent was temporary in order to allow time for technology to develop, no such technology has emerged. After several periods of comments, the FTC stated in March 2006, "the Commission conclude[d] that more secure electronic mechanisms and infomediary services for obtaining verifiable parental consent are not yet widely available at a reasonable cost." (FTC 2006)

According to the Center for Democracy and Training, despite the work of the FTC, the protection of children online is still a serious issue (Jones 2007). To deal with online privacy concerns, the FTC advocates parents stay aware of what children are doing online (Jones 2006). However, it appears parents are not heeding this advice as reports show that 10% of eight to 10 year olds and 21% of 11 to 14 year olds have Internet access in their bedrooms (Roberts et al. 2005). This raises the question as to why parents are not doing more to protect their children. Our purpose is to answer this question by investigating parental awareness of laws and technologies for protection of children's privacy online, and usage of technologies and techniques for parental control.

Technologies For Online Privacy Protection

Online privacy protection has taken two paths: (1) self-regulatory "seals" of approval designed to impart trustworthiness to users and (2) a technical platform (known as P3P) that allows users to set privacy preferences for automatic implementation. Both approaches were developed initially to address adult concerns about online privacy, therefore their inherent limitation is the failure to address the more complex and pressing need of protecting children who lack the sophistication to protect themselves.

Four entities have received FTC approval as safe harbors for providing a methodology for meeting the requirements of the law: PRIVO, Children's Advertising Review Unit (CARU), ESRB Privacy Online, and TRUSTe. A safe harbor involves standards and procedures approved by the FTC. If a business goes through the processes of and adopts the standards of this safe harbor, they will be assumed to have met the requirements of the law. The approved programs are primarily based on seal programs, which comprise a standard agreement to use particular means to obtain a parent's consent, providing notice, payment of fees, audits, and participation in online dispute resolution processes. The website can then post a children's privacy seal, indicating compliance and certification. While seals are designed to stimulate trust and increase use, researchers find consumers do not view them as effective or important (Bélanger et al. 2002; Cranor et al. 2003; NTIA 2002).

Considering the number of children online, it is surprising that no widely acceptable technical solution for verifiable parental consent has emerged since COPPA was enacted. One highly touted, proposed, system for privacy protection is P3P. However, a recent report to the FTC concludes that, in general, the error rate for P3P implementation was unacceptably high, and many policies were out of date (Cranor et al. 2003). Of all the children's sites studied, only 3% used P3P and the privacy policies in these sites were no better than sites not directed toward children. The Thornburgh Committee and the Child Online Protection Act (COPA) Commission, two Congressionally appointed investigative groups, recently concluded that educating and empowering parents to use filtering and other tools is more effective than criminal law at protecting children online (CDT 2007).

Methodology

Given the lack of in-depth literature on parental awareness and use of privacy protection tools, we conduct exploratory research with focus groups of parents with at least one child between the ages of 5 and 13. Focus groups provide a desirable approach to gaining insights into a research domain where limited research has been previously published as they allow researchers to get deeper into the topic of interest by providing more background information about the circumstances of the answer (Krueger 1994).

Respondents

To select participants for this research, we contacted church groups, sporting associations, and parent-teacher associations from different geographical areas. When conducting focus groups, it is normal practice to stop collecting more data when saturation is reached. Saturation occurs when no new information is gained from additional data collection. In the present study, starting with the third focus group, concepts or themes that emerged had all been identified in previous sessions. Nevertheless, a fourth focus group was conducted, at which point no additional findings were made. Therefore, a total of four focus groups were conducted: one with parents from a soccer association, one with parents from a parent-teacher association, and two from church groups from different areas. Each session had three to six people for a total of 18 parents. Table 1 presents respondent demographics.

Table 1. Respondent Demographics

Demographic (n = 18)	**Range**	**Average**
Age (years)	29-48	38.6
Work experience (years)	8-26	16.6
Computer experience (years)	6-27	16.7
Number of children	1-10	4
Computers at home	0-3	1.6
	Categories	**Count**
Gender	Male	4
	Female	14
Education	High School	5
	Two-year college	3
	Bachelor	5

	Graduate	5

Focus Group Procedures and Coding

Prior to conducting the focus groups, a protocol was developed, tested, and modified several times. During the focus group sessions, parents signed a consent form, answered demographic questions, and questions from the protocol. Two researchers attended the sessions. One of the researchers moderated the discussion and probed for further details when appropriate. The sessions lasted on average 60 minutes. The recorded sessions were transcribed into text files and imported into Atlas.ti for data analysis.

An initial list of categories was developed from the focus group protocol and knowledge gained during the focus groups (Miles et al. 1994). The list was revised several times. Once the team agreed on the list of categories, two individuals coded one focus group session each. The coders then met with one of the researchers to compare their coding and discuss differences until agreement was reached on the categories, meanings, and future coding procedures. The coders then coded the remaining transcripts using a revised coding template. The inter-rater agreement was 75.1%, a satisfactory level. Atlas.ti was then used to obtain tabulated results.

Results

Parental Awareness

Legal Awareness

Results indicate that parents are not aware of COPPA and the legal requirement of websites to gain parental consent for collecting personally identifiable information. None of the respondents indicated any knowledge of COPPA. As one individual suggested, parents will try to see if laws are available only if a problem occurs:

> *I think there should be, but I'm not aware … when the problem doesn't come I don't do it, but when the problem does come I do some research…*

Of all the respondents, only two had very vague knowledge of some aspects of the laws. None of the parents knew where to report fraudulent web activity (i.e. to the FTC).

> *I was just thinking the laws about becoming a predator and the laws that are associated with that. So that's basically what I was thinking about the laws. Other than that…*

Tools and Technology Awareness

As discussed before, four safe harbor programs are approved by the FTC for COPPA compliance. We asked respondents to rate their level of knowledge of those programs. As shown in Table 2, parents are not aware of the safe harbor means used by websites to convey their compliance.

Table 2. Awareness Levels of FTC Approved Trust Seals (n = 18)

Ratings	PRIVO	ESRB	CARU	TRUSTe
Never heard of it	17	17	18	16
Vaguely heard of it	1	1	0	2
I know about this but do not use it	0	0	0	0
I have used it once	0	0	0	0
I use it regularly	0	0	0	0

While not aware of the laws and the FTC approved compliance programs, some of the parents recognized some other seals or tools (not specifically privacy protecting tools). In particular, some recognized Verisign and Web Nanny as

demonstrated in Table 3. Verisign provides security measures for sharing sensitive information, and Web Nanny is a content filtering software.

Table 3. Awareness Levels: Distribution of Respondents (n = 13)

Ratings	P3P	AT&T Privacy Bird	Web Nanny	Verisign
Never heard of it	12	11	6	9
Vaguely heard of it	1	2	5	3
I know about this but do not use it	0	0	1	0
I have used it once	0	0	0	0
I use it regularly	0	0	1	1

Overall, it appears that few parents are aware of privacy protection tools or practices available to protect their children's privacy online.

> *So I know that there are some safety features that we can implement that we haven't.*
> *I just vaguely heard about it somewhere, I don't even know where. Just had a conversation or something*

Online Activities Awareness

Finally, regarding what children do online, most parents admit to knowing only some of the sites children go to. None of them knew if merchants do anything to protect their children's privacy online. When asked about whether they believe their children were asked to provide information, most said they believe so, and a few respondents provided examples. Several parents indicated their children were instructed to put the parent's email in when asked.

> *A lot of the motocross ones just for instance you have to put your own email address before it will show you anything.*
> *I think that she likes to go the American girl website and I think on that they ask for their age or that type thing. I tell him to put mine. I mean for that he asks though but they won't give him a lot of … any information until there's an email address.*

Several parents lamented the fact that so many sites their children visit require an email address before the children can access the information they are seeking on those sites.

Perceived Risks

Parents were asked what dangers they believe their children faced on the Internet. While the question was open ended, four parents specifically mentioned predators on the Internet. The other major category that emerged was that most parents indicated they were concerned about their children sharing information online. These concerns were often voiced more towards predators, again, then towards their children's privacy in general. Many parents identified MySpace as a particularly troublesome web site. MySpace is a social networking site that allows individuals to post commentary and pictures.

> *…like a blog and she's just going ahead and typing all this stuff…I was like you can't do this type of stuff. She was telling everything that happened that day. At school, who she talked to, you know the neighborhood she lived in. I mean if someone wanted to target that child she was wide open. It just freaked me out.*
> *That's the problem with MySpace.*

Parental Control

Parents were asked how they control what their children do online and what tools they use to protect their privacy. Responses varied significantly, but we found some key themes. We discuss two main control mechanisms used by parents: technologies and tools, and techniques.

Technologies and Tools

Several parents use passwords as a means to "protect" their children online. Four respondents stated that their computers are password protected, preventing their children from using the computers without their knowledge.

> *My wife and I, and one of us has to physically logon to the computer for our kids to use it. So we already know where we've been and where they've been.*

Other parents stated that they use some form of logging software, meaning that they look at which sites their children visit. At least two parents mentioned warning their children about their ability to see which sites they have visited. Another parent says he looks at the cookies from the sites his children have visited. One parent mentioned the name of the software used: Content Protect.

> *We actually use… 'Content Protect' that actually is password protected and when they go in there, they have to put a password in that actually identifies at least who is online. That program actually records everything that happens. It can record all their IMs. It records what websites they see. It also can restrict them as to what timeframes they can be on the internet. And ah omm but you know… it still doesn't automatically protect them from identifying themselves and we've had some discussions with our older ones particularly about that about putting identifying information on. So that they are aware of the dangers that exist with that.*

When this parent was asked how he found out about this tool, it became clear the parent made an extra effort to find tools when he became aware of threats.

> *I was concerned about what my kids and the availability they had of what was online so I wanted at least you know to say its hard to keep track …of what [they] are doing all the time… So I just started doing web searches and what tools are out there to be able to do that. I felt for me Content Protect was the best tool. I did look at Web Nanny as well…*

Overall, few parents knew or used tools beyond password protection. As one parent explained, it is often the effort to install and manage the software that prevents them from using it. Other times, parents do not have technical expertise to do this. As seen in the second quote, one parent believed that Norton Antivirus would protect their children from bad content on the Internet.

> *Web Nanny. We've used it before. And I don't know in switching different computers it didn't get loaded on the last one, the computer that we have. Don't know what happened to it.*
> *We have the virus scan and things like the protection that is supposedly with the computer and upgraded the security like Norton.*

Techniques

While not often using technologies and tools, parents do use various techniques that are not computer-related to have some level of control over their children's activities and privacy online. Five of the 18 respondents suggested that the computers are in plain view in their home, limiting what children would do. However, as one parent suggested, that is often not considered enough.

> *… 2 desktops are in 1 room so that I can watch and those are the ones I allow the kids to get on.*
> *… parental supervision and software but there needs to be more because you can't, I've got 5 children and I can't be everywhere.*

The real issue for many of the parents is that they do not actually control what their children do online, but they rely on trusting that their children will do the right things, according to parental instructions. A surprising number of respondents indicated that while they trust their children they somehow know that they shouldn't.

> *My daughter… she asks me to use the computer. For what kind of purpose she will tell me and I say OK and she will go ahead. And usually I think she will do anything she will ask my consent to do anything. Right now its OK, but in the future I'm afraid that once she found something that's interesting or that made her very very enthusiasm and I would lose control about that. And I can't promise that she won't let out any information that I don't want her*

to let out. So although I just told her not to have your personal information given out. But I don't know about the future.

Trust I guess. Our computer is downstairs. But again we can always back into her room and check it. I know all her passwords to get online for her email or anything like that.
We're just too trustworthy I think. We just expect our kids to walk that line.

Usage Factors

Finally, parents were asked what would make them start to use a tool that would protect their children's privacy online. The analysis revealed several key factors, as illustrated in Table 4.

Table 4. Usage Factors

Parents will use a privacy protection tool if …	**# of comments**	**% of comments**
1 … it requires little effort (easy to use)	16	43%
2 … it is easy to modify its settings	5	14%
3 … it is needed because the regulations in place protect their child	3	8%
4 … log files are available (but can be turned on and off)	3	8%
5 … it gives them more control over the consent they give for sites their children visit	2	5%
6 … it is efficient to use (cost – benefit)	2	5%
7 … it provides a list of pre-approved sites (convenience)	2	5%
8 … it gives them more control over their children's privacy	1	3%
9 … they believe that others they know are using it	1	3%
10 … it is also implemented in schools	1	3%
11… it is downloadable (can't be lost)	1	3%
Total	37	100%

Discussion

The United States Congress has established two panels with the responsibility of investigating how to best protect children online. Both panels reached the conclusion that laws and regulations would be ineffective, and that the best ways to protect children online would be through education and technology (Jones 2007). Although our findings support these conclusions, they also illustrate that parents are unaware of the laws, regulations, and technologies available to protect their children's privacy online.

The results from the focus groups provide insights into what causes parents to use techniques or technological tools to protect their children's privacy. The emergent model from the data analysis consists of technology adoption factors, behavioral adoption factors, and awareness factors that lead to privacy protection behaviors, both technological and non-technological (see Figure 1). The following section describes this emergent model in further detail, giving examples from the focus groups to explain how each construct fits in the model.

Privacy Protection Behaviors

Two privacy protection behaviors were identified as being used by parents – technological and non-technological. Use of privacy protection technology is currently not performed by most parents but parents use various techniques for trying to control their children's privacy. The model, therefore, contains both technological tools and techniques for protecting children's privacy.

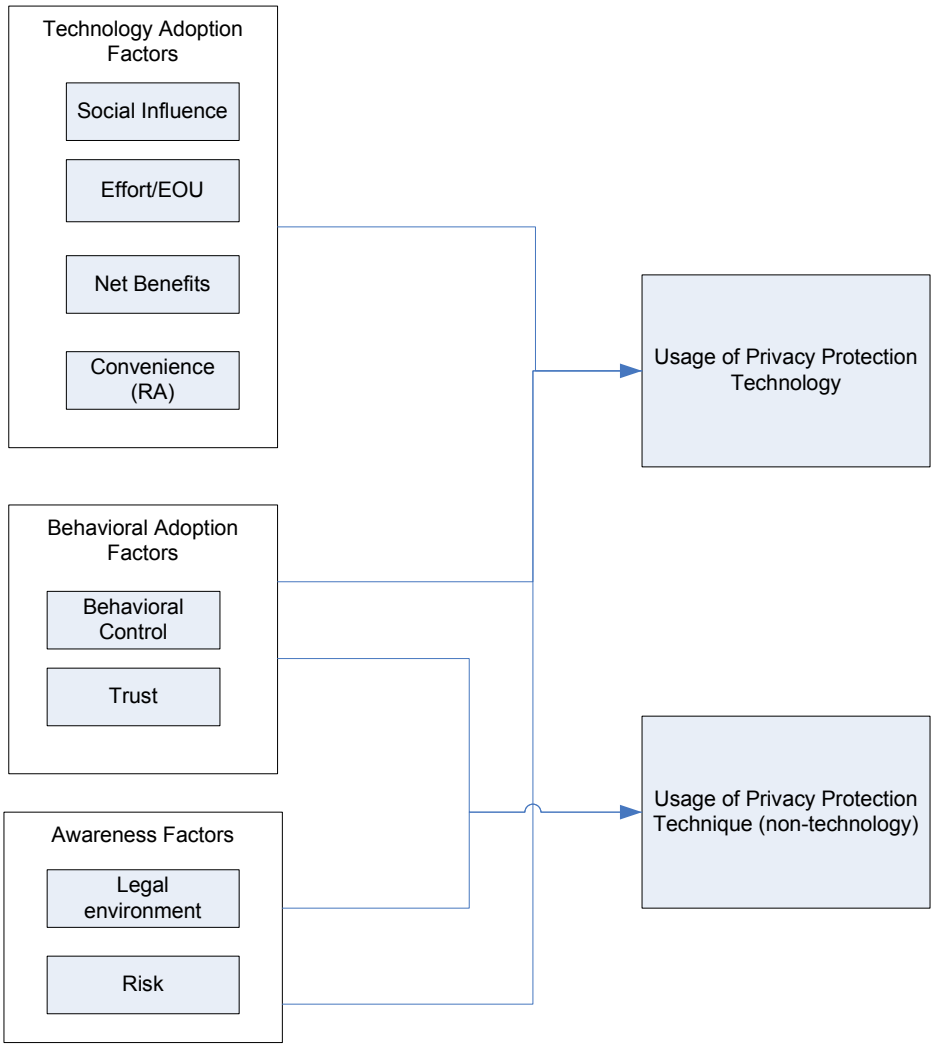

Figure 1. Emergent Privacy Protection Model

Technology Adoption Factors

Technology adoption models regularly show that individual traits lead to behavioral intention which then leads to use of a technology (Venkatesh et al. 2003). In the focus groups a number of technology adoption factors emerged – social influence, effort, net benefits, and relative advantage. In the proposed model, these technology adoption factors are expected to impact use of privacy protection technologies and tools, but not use of privacy protection techniques (non-technology based).

Social Influence

Parents in our focus groups indicated that one way to get them to use a privacy protection tool would be through the influence of others. This is consistent with prior research where social influence is predicted to affect technology usage. Social influence can be defined as the degree to which an individual perceives that others who are deemed important to him or her believe that he or she should use the privacy protection tool (Venkatesh et al. 2003).

> *If this was something like the don't drink, don't smoke, don't talk to strangers ads that came on TV or that was distributed through schools. Or the schools have educational websites that they let the kids go to during rainy days at recess. If this was something that the kids got excited about and were like hey! Like McGruff or Smokey the Bear or anything else. Mom dad this [tool] I heard about it at school we really need to put it on the computer. What better way to get us to do it.*

Effort/Ease of Use

Parents commented many times that in order for them to use a tool to protect their children's privacy it needed to be easy to use (mentioned 16 times) and easy to modify when needed (mentioned 5 times). Examples of these comments are provided below. Again, this is consistent with several technology adoption models, such as the Technology Acceptance Model (Davis 1989) or Unified Theory of Acceptance and Use of Technology (Venkatesh et al. 2003). Effort, or ease of use, is defined as the degree of ease associated with the use of the technology (Venkatesh et al. 2003).

Yeah same reason we forget to use everything else. We just…we work with multiple computers it's too hard to keep up with stuff.
… if it isn't working or if it is too difficult to get into on a regular basis it just becomes a nuisance.

Net Benefits

Parents indicated the benefit of using a technology to protect their children's privacy was impacted by the cost of acquiring that technology. If a protection privacy tool would be made available for free, they thought it was an easy decision. While cost could be considered a factor by itself, the idea of cost versus features is better captured by the net benefits construct, which focuses on the balances of positive and negative impacts of the technology (DeLone et al. 2003).

R4: I think you'd have to compare the cost to what else is out there. And the features to what else is out there.
F1 (facilitator): What if its free?
R4: I think at that point it's a slam dunk. I mean if its free…

Convenience/Relative Advantage

Parents mentioned a privacy protection tool would have to have certain features, such as log files that can be turned off (so children would not see their parents' logs), lists of pre-approved websites (so they would spend less time approving sites at first), and a downloadable product (so they could get it again easily of they "lost it"). These convenience factors can be represented by the relative advantage construct, which refers to the perception that a new innovation is better than what was used before it (Moore et al. 1991; Venkatesh et al. 2003).

At least something you can download. I lost the software for the other somewhere.

Behavioral Adoption Factors

Behavioral adoption describes why people perform certain behaviors (Fishbein et al. 1975). Two behavioral adoption factors became apparent during our focus groups – behavioral control and trust. Behavioral adoption factors are expected to impact both the use of privacy protection technologies and the use of privacy protection techniques.

Behavioral Control

The behavioral control construct refers to the internal and external constraints on a person's behavior and encompasses self-efficacy (Taylor et al. 1995; Venkatesh et al. 2003). Self-efficacy is the confidence a person has in their ability to use technology to complete a certain task (Compeau et al. 1995; Venkatesh et al. 2003). Parents indicated their desire for control over both their children's privacy and the consent they give to websites (see Table 4). However, parents often indicated they wanted to use software to protect their children's privacy but didn't know how.

No, but I want to. As she gets older I want to. I don't know how to though.

Trust

In the study, trust appeared to impact use of privacy protection tools and techniques in two very different ways. On the one hand, parents indicated that they trusted their children, and therefore did not feel the need to use privacy protection

tools and techniques. On the other hand, parents indicated that they needed to trust the software to watch what their kids were doing. Two types of trust can then be considered important to the use of privacy protection tools. Institution-based trust (IBT) refers to *an individual's perceptions of the institutional environment, including the structures and regulations that make an environment feel safe* (McKnight et al. 2002). In this case, IBT refers to the privacy protection tool and its ability to meet regulations. Characteristic-based trust (CBT) refers to *one's belief in the integrity and ability of the trustee* (McKnight et al. 2002). In this case, CBT involves trust of the parent in his children to be aware and capable of dealing with threats to their own privacy.

> *Software …. Anytime there's always a way around things. A glitch in something. I have a hard time trusting something like something at all any other mechanism to watch what my kids are doing. I have a hard time trusting it to do what it says it does.*

Awareness Factors

As previously discussed, parents are not aware of the laws or risks relating to children's privacy. Without an understanding of either of these aspects it is unlikely that parents would take necessary measures to protect their children's privacy. As such awareness is a necessary determinant of both use of privacy protection technology and use of privacy protection techniques. The results confirm this as both awareness and usage were low.

Limitations

As with any research this study has its own set of limitations. One issue with focus group research is the potential that not all individuals will share their perspectives on the issues being discussed due to the presence of dominant or passive individuals. To address this limitation the focus groups were facilitated by a trained researcher who prevented individuals from dominating the conversations and drew comments out of those who were more passive.

Another potential limitation of focus group research is the personal dynamics caused by individuals that are connected by means of work or other social circumstances resulting in certain individuals withholding comments. In this study, such behaviors were not observed. The facilitator was able to draw meaningful discussions out of all individuals of the focus groups.

Future Research

The next step in this research is to test the predictive value of the emergent model. To accomplish this, a large-scale survey will be conducted with a wide diversity of parents.

Conclusion

As the number of children using the Internet continues to grow, protecting their privacy becomes an ever more pressing issue. Parents have a key role to play in ensuring children are protected. Yet, as demonstrated in this study, few parents are aware of the laws and technologies available to perform this. This study proposes an emergent framework as a result of focus groups conducted with parents. The framework can serve as a starting point to explore factors that can help ensure parents are aware of laws and technologies, and use privacy protection tools for their children in the online environment.

Acknowledgement

This research is supported in part by NSF grant CNS-0524052.

References

Bélanger, F., Hiller, J., and Smith, W.J. "Trustworthiness in E-Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11:3/4) 2002, pp 245-270.

CDT "Child Safety and Free Speech Issues in the 110th Congress," Center for Democracy and Technology, Washington DC, p. 10.

Compeau, D.R., and Higgins, C.A. "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly* (19:2) 1995, p 189.

Cranor, L.F., Byers, S., and Kormann, D. "An analysis of P3P deployment on commercial, government, and children's Web sites as of May 2003," AT&T Labs-Research, Florham Park, NJ.

Davis, F.D. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly* (13:3) 1989, pp 319-340.

DeLone, W.H., and McLean, E.R. "The DeLone and McLean model of information systems success: A ten-year update," *Journal of Management Information Systems* (19:4) 2003, p 9.

Fishbein, M., and Ajzen, I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research* Addison-Wesley Publishing Company, Reading, MA, 1975.

FTC "Retention of Rule without Modification," 2006, p. 35.

Jones, K.C. "CDT Analyzes Data Retention, Other Proposals For Protecting Kids Online," in: *Information Week*, 2007.

Jones, P.H. "Prepared Statement of the Federal Trade Commission Before the Subcommittee on the Oversights of the Committee on Energy and Commerce," Washington, DC, p. 9.

Kawamoto, D. "VeriSign works to ID kid surfers," in: *Cnet News*, 2004.

Krueger, R.A. *Focus Groups: A Practical Guide For Applied Research*, (2 ed.) SAGE Publications, Inc., Thousand Oaks, CA, 1994, p. 255.

McKnight, D.H., Choudhury, V., and Kacmar, C. "Developing and Validating Trust Measures for E-Commerce: An Integrative Approach," *Information Systems Research* (13:3) 2002, pp 334-359.

Miles, M.B., and Huberman, A.M. *Qualitative Data Analysis: An Expanded Sourcebook* Sage Publications, Thousand Oaks, CA, 1994.

Moore, G.C., and Benbasat, I. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3) 1991, pp 192-222.

NTIA "A nation online: How Americans are expanding their use of the Internet," in: *http://www.ntia.doc.gov/ntiahome/dn/index.html*, Economics and Statistics Administration, 2002.

Roberts, D.F., Foehr, U.G., and Rideout, V. "Generation M: Media in the Lives of 8 - 18 Year Olds," p. 145.

Taylor, S., and Todd, P.A. "Understanding Information Technology Usage - a Test of Competing Models," *Information Systems Research* (6:2), Jun 1995, pp 144-176.

Turow, J. "Privacy policies on children's Websites: Do they play by the rules?," *The Annenberg Public Policy Center of the University of Pennsylvania Report Series No. 38*), March 2001.

Venkatesh, V., Morris, M., Davis, G., and Davis, F. "User acceptance of information technology: Toward a unified view," *MIS Quarterly* (27:3) 2003, pp 425-478.