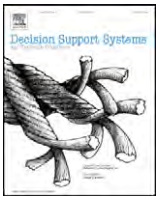
Decision Support Systems 54 (2013) 1161–1173

Contents lists available at SciVerse ScienceDirect

Decision Support Systems

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



POCKET: A tool for protecting children's privacy online ☆

France Bélanger [a], Robert E. Crossler [b,*], Janine S. Hiller [c], Jung-Min Park [d], Michael S. Hsiao [d]

[a] 850 Drillfield Drive, Suite 3007, Blacksburg, VA 24061–0101, USA
[b] PO Box 9581, Mississippi State University, Mississippi State, MS 39762, USA
[c] 850 Drillfield Drive, Suite 2120, Blacksburg, VA 24061–0221, USA
[d] 1185 Perry St. Room 302, Blacksburg, VA 24061–0111, USA

ARTICLE INFO

Article history:
Received 3 August 2011
Received in revised form 12 September 2012
Accepted 11 November 2012
Available online 19 November 2012

Keywords:
Information privacy
Privacy
COPPA
Children
Design science
IT artifact

ABSTRACT

Children's privacy in the online environment has become critical. Use of the Internet is increasing for commercial purposes, in requests for information, and in the number of children who use the Internet for casual web surfing, chatting, games, schoolwork, e-mail, interactive learning, and other applications. Often, websites hosting these activities ask for personal information such as name, e-mail, street address, and phone number. In the United States, the children's online privacy protection act (COPPA) of 1998 was enacted in reaction to widespread collection of information from children and subsequent abuses identified by the Federal Trade Commission (FTC). COPPA is aimed at protecting a child's privacy by requiring parental consent before collecting information from children under the age of 13. To date, however, the business practices used and the technical approaches employed to comply with COPPA fail to protect children's online privacy effectively. In this paper, we describe the design of an automated tool for protecting children's online privacy, called POCKET (Parental Online Consent for Kid's Electronic Transactions). The POCKET framework is a novel, technically feasible and legally sound solution to automatically enforce COPPA.

1. Introduction

A paramount concern of individuals using the Internet is the protection of their privacy. Recent surveys show that awareness regarding personal privacy is growing. A Harris poll designed by Privacy & American Business, a non-profit company that works with businesses on privacy issues, and sponsored by Microsoft found that 35% of Americans had "very high privacy concern" and 65% had refused to register at an e-commerce site because of privacy concerns. While 60% decided not to patronize a site due to doubts about the company's policies, 7% had filed a complaint regarding misuse of personal information [10]. Further, government regulations exist to provide legal protections for people's online privacy [40]. If people are concerned about their own privacy, it can be expected that they are equally or even more concerned about the online privacy of their children. Psychologically speaking, children need protection from the dangers of sharing personally identifiable information online because they are socially immature and naïve [20]. Conversely, they are correspondingly sophisticated about the use of the Internet and computers, frustrating the busy and less technological savvy parent trying to protect their child online [20]. To put this in other words, children know how to use the technology, including the Internet, but their parents either do not have the time or technical know-how to adequately protect their privacy online. This refers to the concept of parental computer self-efficacy.

Recognizing the importance of protecting children's privacy on the Internet, the Children's Online Privacy Protection Act of 1998 (COPPA) enacted in the United States requires parental consent before websites can collect information from children under the age of thirteen. The Federal Trade Commission (FTC) has adopted regulations to enforce COPPA. Unfortunately, technology has not been developed to offer strong protection for children's privacy and has resulted in websites facing civil penalties due to COPPA compliance issues [14]. An example of this problem is the case of Xanga.com [13], an interactive social networking site that was fined $1 million dollars by the FTC for failing to effectively implement parental consent for children to use the site. Its failure was massive, with over 7 million children accessing the site, creating profiles with birth dates indicating they were 13. Further, Xanga.com failed to notify parents about their information collecting practices or provide parents access to and control of the information collected from children. Social networking sites, where personal information abounds, can pose a special danger to children who may share offline identifying information that will allow them to be contacted or

☆ Various sections of this work have been presented at the following conferences: America's Conference on Information System (AMCIS) 2007, Decision Sciences Institute (2008), and International Conference on Security and Management (SAM 2008).

* Corresponding author at: PO Box 9581, Mississippi State University, Mississippi State, MS 39762, USA. Tel.: +1 662 325 0288; fax: +1 662 325 8651.
E-mail addresses: belanger@vt.edu (F. Bélanger), rob.crossler@msstate.edu (R.E. Crossler), jhiller@vt.edu (J.S. Hiller), jungmin@vt.edu (J.-M. Park), mhsiao@vt.edu (M.S. Hsiao).

0167-9236/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2012.11.010

tracked. By implementing parental control over the personally identifiable information that a child can share, COPPA intends to empower parents to protect their children. Yet, as the Xanga.com case shows, the protocol as it now exists requires a website to contact the parent for consent, and children are adept at circumventing website procedures.

The goal of this research is to follow design science guidelines [19,27] to design an artifact called POCKET (Parental Online Consent for Kid's Electronic Transactions) that provides a reliable, trustworthy technology option for obtaining verifiable parental consent as required by COPPA. POCKET is designed to allow a parent to control access unless the website consents to the information collection parameters set by the parent. POCKET provides an easy-to-use interface for parents to configure privacy choices for their children, and then automatically enforces these policies. By maintaining an activity log of the interaction with the websites, it provides a way to ensure accountability in case of disputes. The development of POCKET was guided by input from focus group sessions. The proposed tool is described further in this paper. This research provides several contributions to the literature. First, it uniquely combines expertise and theory from the fields of business law, computer engineering, and information systems to develop a tool to provide accountability and enforcement of COPPA. Through explicating the kernel theories implicitly interwoven into POCKET, we set the stage for future broader compliance with COPPA and other regulated Internet activities. Second, POCKET extends work on the Platform for Privacy Preferences project (P3P). Third, the research provides a further examination of children's privacy online, including identification of factors influencing parents' use of software to protect their children's privacy online, and a description of what parents need to do to protect children's privacy. Fourth, the design shows how researchers have to work around parents who are not tech-savvy to provide usable solutions. Finally, the research demonstrates how design science can be used to provide practical and relevant tools for individuals, filling an identified gap in the privacy literature [4].

The paper is organized as follow. First, we discuss the theories and requirements for POCKET from legal, technical, and behavioral perspectives in the next section. The third section discusses the actual design of POCKET. This is followed by the evaluation of POCKET from the legal, technical and behavioral standpoint. The fifth section presents a discussion of POCKET as an IT artifact and how the project met the design science guidelines. This is followed by concluding remarks, including limitations and future research.

2. Theoretical foundations for the design of POCKET

The POCKET project was initiated in response to the lack of technically viable solutions for the implementation of the COPPA legal requirements. For the design of POCKET, however, the research team had to consider not only the legal requirements, but also a set of technical and behavioral requirements. To illustrate the process of how the requirements as well as overarching theories informed this development process, we draw on the design science framework provided by Kuechler and Vaishnavi [24] and present our discussion of kernel theories, requirements, and design principles following the structure offered by Ngai et al. [34]. Kuechler and Vaishnavi's framework demonstrates how, in the development of an artifact, theory is tacitly included in the product of all design science research. Following this framework and other design science work, we drive the development of our artifact beginning with kernel theories that led to the identification of the requirements for POCKET, which ultimately led to the design principles that guided the development of our artifact. Kernel theories from the three reference disciplines drove the development of POCKET: legal, computer science, and information systems. In this next section, we further describe the kernel theories, requirements, and design principles that informed POCKET's design.

2.1. Legal environment

2.1.1. Legal kernel theory

Legal requirements refer to regulations mandated by COPPA and represent the overarching requirement this design had to meet. The Children's Online Privacy Protection Act of 1998 (COPPA) enacted in the United States requires parental consent before websites can collect information from children under the age of 13. COPPA seeks to protect children by giving parents control over what information their children can share with websites.

2.1.2. Legal requirements

The legal requirements of COPPA in general have been widely discussed [20], so we only briefly review them. COPPA regulations adopted by the FTC provide a list of what can be considered personally identifiable information for children. In addition, COPPA provides further requirements regarding notice, because for parents to protect their children, they must be aware of website information collection practices and their right and ability to control information collection. Parents must then explicitly give consent for websites to collect information from their children. Verifiable parental consent is one factor of COPPA that, technologically, has proven to be one of the most challenging to implement.

Verifiable consent as required by COPPA includes "(a)ny reasonable effort (taking into consideration available technology)." Initially, a temporary sliding scale of various methods was adopted by the FTC until technology was created that could provide a more sophisticated, reliable, and cost-efficient manner to obtain consent. The sliding scale allows websites to decide the method they use for obtaining parental consent for collecting the child's personal information [12]. The website can employ a cost effective method in obtaining parental consent based on the site's data use policy. For example, the FTC allows for a less reliable method, E-mail Plus (uses an e-mail message to get parental consent), if the website uses the data gathered for internal purposes only. The FTC requires a more reliable method for gaining parental consent if the merchant shares the data gathered with third parties. These methods include using a print-and-send consent form, a credit card transaction, a toll-free telephone number staffed by trained personnel, a digital certificate using public key technology, or an email with a password or PIN obtained by one of the above mentioned methods [12]. The FTC hoped that technological advances would provide a more sophisticated, reliable, and cost efficient manner to obtain consent. However, because the technology did not emerge, the FTC made the sliding scale approach permanent.

An additional requirement of COPPA is for websites to not knowingly encourage children (under the age of 13) to give information that is not necessary for participation on the website. In other words, websites should not entice children to provide information in order to be able to access the site, unless needed for business with documented purposes. Finally, COPPA requires websites to protect and maintain the accuracy and security of the information they are allowed to collect. In summary, the legal requirements of COPPA include the following:

1. Provide notice of information collection practices, including use and disclosure practices.
2. Obtain prior verifiable parental consent for the collection, use, or disclosure of the information. Parents should have the ability to refrain from giving consent.
3. Facilitate parental access to information collected, the right to delete the information, and the ability to prohibit further collection. Parents should also be able to change or withdraw consent.
4. Refrain from conditioning a child's participation in online activities on disclosing information unless it is reasonably necessary.
5. Protect and maintain the accuracy and security of the information collected and/or stored.

The types of information that can be considered personally identifiable under COPPA include a wide variety of data elements. Fig. 3, in Section 3.3, shows the types of information as required by COPPA, and those that are implemented in POCKET. It should be noted that the key aspect missing from the implementation of COPPA was a robust method of obtaining parental consent. POCKET focused on this aspect of the implementation rather than the disclosure aspect.

2.1.3. Legal design principles

The legal requirements identified above led to the identification of design principles that needed to be followed to ensure that the resulting POCKET artifact would meet the requirements that the law mandates. The resulting design principles are listed below, which correspond with the same numbered requirements above.

1. POCKET should provide a way to verify the privacy practices of websites.
2. POCKET should automate the process of parents providing consent to the release and use of their children's information at a granular level as it matches the parent's predefined preferences.
3. POCKET should provide a method for parents to review information that has been provided to websites and notify websites if the information should be deleted.
4. This legal requirement is beyond the control of an artifact such as POCKET and is a behavioral decision of website merchants.
5. POCKET should properly secure information that it contains, as well as provide accurate information to website merchants it shares information with on the parent's behalf.

2.2. Technical environment

2.2.1. Technical kernel theories

The kernel theories result from the contextual environment in which POCKET is meant to operate (e.g., commercial websites, secured transmissions, diversity of user environments, etc.). As a result, the theories that informed the technical requirements were tacitly embedded in existing software designs [24], such as cookies, anonymizers, software controls, privacy policies, and seals. Over the years, researchers have proposed these various tools and techniques to protect consumer privacy online. While not directly related to children's privacy, each of these technologies has tried to address privacy issues on the Internet. The tools, however, have not been successful at addressing all of the privacy issues previously discussed, and none of them is able to completely address the legal requirements of COPPA.

2.2.1.1. Cookies and anonymizers. The advent of cookies as an extension to the stateless HTTP protocol standard allowed web sites to tag a browser with information that would be available to the server when the user returns. Cookies provide a method to track the visitor of a website, and websites started storing this tracking information for extended periods. The use of cookies raises privacy concerns [22] when third party cookies started linking collected browsing history with other gathered information [11]. To protect user privacy, browser companies including Microsoft, Mozilla, Google, and Apple provide privacy control features in browsers to limit the collection of information through cookies. Anonymizers offer anonymous web surfing by acting as an intermediary between the user and the website. Most anonymizers prevent the website from tracking the client's IP address or placing cookies in the viewer's computer. These are true privacy-enhancing technologies [11], because they remove identifying information completely. In the design of POCKET, cookies and anonymizers suggest that we need to provide as much automation as possible.

2.2.1.2. Privacy policies. Companies and websites may use a privacy policy to provide notice to consumers of the website's information collection practices. The privacy policies may outline the kind of information being collected, the purpose for collecting the data, companies with which this information is shared, whether the consumer has access to the data, online contact information, and so forth. Generally speaking, outside of COPPA and topic specific laws, there is no requirement for a website to post a privacy policy. Legal and privacy experts prepare the policies, which include terminologies that make it difficult for ordinary consumers to read and understand. The Platform for Privacy Preferences project (P3P) created by the World Wide Web Consortium (W3C) was aimed at creating a machine-readable, common vocabulary for identifying privacy practices. The P3P policies are expressed in the eXtensible Markup Language (XML) format [42]. P3P enables the websites to express their privacy policies in a standardized machine-readable format so that automated tools (or user agents) can interpret them [7,25]. P3P also includes syntax, called compact P3P, to represent a site's data practices for cookies. This feature is used by several existing browsers to make decisions regarding blocking or allowing cookies [5]. The Internet Explorer 7 (IE7) web browser (and later versions) implements a P3P based cookie management system [29]. The IE7 privacy feature filters cookies using compact P3P and the user's privacy settings. IE7 allows users to perform coarse cookie control by selecting from among six different preconfigured settings (from block all to accept all). Several other browsers have similar privacy controls based on compact P3P. P3P user agents inform the consumer of the site's practices so that the user can make an informed decision regarding the use of a particular website. Privacy Bird [8] is the most advanced, easy to use and open-source user agent implemented by AT&T Labs for visualizing the privacy policies. The Privacy Bird displays an icon of a bird that changes color, and provides vocal feedback when the preferences of the client and website policies match (differ). The user has the option to continue (stop) using the website.

2.2.1.3. Software controls. Several parental control packages that protect children from inappropriate content on the Internet are available today. Tools include browser add-on modules, dedicated software, and operating system features that help prevent children from accessing such materials online. These tools can be used to monitor the child's activities on the computer and Internet, but do not address privacy issues. Microsoft's latest operating systems, including Windows Vista and Windows 7, provide more advanced parental control features that can be used along with Microsoft's latest browser, Internet Explorer 8 (IE8) [28]. Parents can restrict their children to playing particular games, running specific programs and visiting specific websites. In addition, parents can configure time limits on the child's daily computer use. Net Nanny (http://www.netnanny.com/) is an example of parental control software that allows parents to monitor the child's activity logs, set time limits on computer use, and block access to certain software. Net Nanny also blocks sending a set of configurable private information in outbound communication. The Parental Control Toolbar (http://www.parentalcontrolbar.org/) is another privacy control feature available as an extension to various browsers. It helps parents prevent children from viewing adult-oriented websites. The toolbar assumes that websites voluntarily label the pages based on the Internet Content Rating Association's (ICRA) vocabulary. The Parental Control Toolbar uses these labels to decide whether the website contains suitable content and blocks websites containing inappropriate content.

2.2.1.4. Trust seals. In an attempt to self-regulate regarding privacy concerns in general, industry groups developed trust "seals" targeted at reassuring consumers that the companies displaying the seals abide by the seal program's privacy rules. Examples of programs include TRUSTe (http://www.truste.org/), BBBOnline (http://www.bbb.org/us/bbb-online-business/), and the CPA Web-Trust (http://www.webtrust.net/). Most current solutions for meeting the requirements of COPPA primarily have been based on similar seal programs

rather than on technical solutions. These programs generally comprise a standard agreement by a website to protect children's privacy, the payment of a fee, routine audits, and an online dispute resolution process. Upon completion of this process, the website is allowed to post a children's privacy seal, which indicates to the users that the site is compliant and certified. In theory, seals are designed to induce brand-like recognition and stimulate trust in the website, therefore increasing the chance that a person will use the site.

2.2.2. Technical requirements

The technical requirements for POCKET were derived from a combination of legal factors (e.g. secured information requires encrypted transmissions), technical factors due to the working environment (e.g. websites require the use of Internet protocols), and technical factors that make use of technically feasible existing solutions (e.g. P3P provides privacy policy information that can be used by POCKET).

With respect to the working environment, the design of POCKET must take into account that parents are the users of the system. In other words, the system will have to be easy to implement and use (Requirement 1). In addition, POCKET needs to be developed for a popular environment first, such as Internet Explorer, which is more likely to be widely used (Requirement 2).

In terms of the working environment for feasible solution, POCKET needs to make use of cookies and anonymizers where possible to provide as much transparency and automation as possible, facilitating the job of parents in making use of the software (Requirement 3). POCKET also needs to leverage prior P3P technology (Requirement 4). Many P3P user agents were developed during the standardization process of P3P. However, there are implementation problems with P3P, with research showing errors in policy implementation, violations of policy, and incomplete policies [6]. This has led researchers to recommend that a third party be used to certify compliance. Even if P3P could be implemented in a dependable manner, the privacy language constructs are not fine grained enough to address the specific choices that a parent would make regarding the exact information that a website could or could not collect or share. Lastly, and most importantly, P3P does not incorporate any method for asserting the parent's consent over the child's information. Nevertheless, POCKET can use the basic concepts of P3P and improve on them. A final technical environment to consider when establishing the requirements for POCKET is the use of the control toolbars in prior software, which shows the need to ensure that parents are given controls over the tool (Requirement 5).

2.2.3. Technical design principles

Based on the above review of kernel theories, existing solutions, and requirements, the research team established a set of design principles for the development of the POCKET prototype.

Requirement 1: The system will have to be easy to implement and use.

Design Principle 1.1: POCKET should be easily downloadable once parents are registered.

Design Principle 1.2: POCKET should be easy to install using a self-extracting file.

Design Principle 1.3: The User Interface should be graphical and easy to navigate with a combination of menu items, dialog boxes, and easy to interpret error messages.

Requirement 2: The prototype should be developed for a popular environment.

Design Principle 2.1: POCKET should be developed initially for Internet Explorer using the Browser Helper Object (BHO) tool.

Requirement 3: The POCKET prototype should provide as much transparency and automation as possible.

Design Principle 3.1: The transaction phase (whether the transfer of information is approved or not) should be transparent to parents once POCKET is installed and working.

Design Principle 3.2: POCKET requires secured transmissions of information between the parents, website, and trusted third party machines.

Requirement 4: POCKET needs to leverage prior P3P technology.

Design Principle 4.1: POCKET should automatically compare the Privacy Preference File from POCKET with the website's privacy practices file using P3P User Agent concepts.

Requirement 5: POCKET should give parents control over the tool.

Design Principle 5.1: POCKET should allow parents to modify settings as desired.

Additional requirement: POCKET needs to be developed in a structure, phased approach.

Design Principle 6.1: POCKET should include four phases: registration, installation, transaction, and post-transaction phases.

2.3. Behavioral environment

2.3.1. Behavioral kernel theories

The behavioral environment refers to the need for POCKET to be operable by parents (e.g., who may not be technically savvy, who may be unwilling to spend time using and learning about the software, etc.) and was informed by a wide set of kernel theories such as Technology Adoption Model, Concern for Information Privacy, and Trust.

2.3.2. Behavioral requirements

Prior to the design of the POCKET tool, we developed a mock-up of POCKET to show to potential users (parents) to receive in-depth feedback on the requirements regarding the usability of such a tool. In order to do this, we conducted four focus groups of parents with at least one child between the ages of five 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 [23].

2.3.2.1. Focus groups procedures. Prior to conducting the focus groups, a mock-up was developed, tested, and modified several times. To select participants, we contacted church groups, sporting associations, and parent-teacher associations from different geographical areas. The four focus groups were as follows: 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. During the focus group sessions, parents signed a consent form, answered demographic questions, and questions from the moderator. 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 min. Table 1 presents demographics.

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 [30]. 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. Cohen's kappa was 75.1%, a satisfactory level. Atlas.ti was then used to obtain tabulated results. The focus groups provided

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

insights into parental awareness of laws, tools, and privacy issues on the Internet, as presented in a previous conference paper (withheld for anonymity in review). In addition, parents described factors that would make them start to use a tool that would protect their children's privacy online. Those factors, presented in Table 2, were identified as requirements of POCKET when they were technically feasible (noted by a #).

2.3.3. Behavioral design principles

The requirements identified in Table 2 result in the following design principles. It should be noted that some of the design principles noted as behavioral design principles overlap with previously identified legal and technical design principles.

1. POCKET should be easy to use (requirement 1, 2, and 7).
2. POCKET should meet legal requirements (requirement 3).
3. POCKET should create log files, to be utilized at the parent's discretion (requirement 4).
4. POCKET should provide increased control over information released by children (requirement 5 and 8).
5. POCKET should provide maximum value at a minimal cost (requirement 6 and 11).

2.4. Summary of design principles

Table 3 presents a summary of the design principles for POCKET based on the legal, technical, and behavioral kernel theories and requirements discussed in this section.

Table 2
Usage factors → requirements.

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%

These factors are to be included in the design of POCKET.

Table 3
Design principles.

Environment	Design principle
Legal	POCKET should provide a way to verify the privacy practices of websites.
	POCKET should automate the process of parents providing consent to the release and use of their children's information at a granular level as it matches the parent's predefined preferences.
	POCKET should provide a method for parents to review information that has been provided to websites and notify websites if the information should be deleted.
	POCKET should properly secure information that it contains, as well as provide accurate information to website merchants it shares information with on the parent's behalf.
Technical	POCKET should be easily downloadable once parents are registered.
	POCKET should be easy to install using a self-extracting file.
	The User Interface should be graphical and easy to navigate with a combination of menu items, dialog boxes, and easy to interpret error messages.
	POCKET should be developed initially for Internet Explorer using the Browser Helper Object (BHO) tool.
	The transaction phase (whether the transfer of information is approved or not) should be transparent to parents once POCKET is installed and working.
	POCKET requires secured transmissions of information between the parents, website, and trusted third party machines.
	POCKET should automatically compare the Privacy Preference File from POCKET with the website's privacy practices file using P3P User Agent concepts.
	POCKET should allow parents to modify settings as desired.
	POCKET should include four phases: registration, installation, transaction, and post-transaction phases.
Behavioral	POCKET should be easy to use.
	POCKET should meet legal requirements.
	POCKET should create log files, to be utilized at the parent's discretion.
	POCKET should provide increased control over information released by children.
	POCKET should provide maximum value at a minimal cost.

3. Design of POCKET

Based on the legal, technical, and behavioral design principles presented in the previous section, the technical team designed a prototype of POCKET in two phases, alpha and beta. The paragraphs below present the final POCKET design.

3.1. The POCKET framework

The POCKET framework utilizes and extends the P3P framework by (1) incorporating a trusted third party (TTP) during interaction, (2) extending the merchant policy to include data elements as required by COPPA, including the use and handling of data collected, and (3) automating exchange of personal information between the client and server. The POCKET user agent allows merchants to identify the client as a child and automatically obtain parental authorization for information collected.

Mont and Bromhall [31] and Mont et al. [32] proposed increased user control over the disclosure of information and merchant accountability for using the data collected. Our technical solution extends this work by employing a stronger mechanism for ensuring merchant accountability. We employ a four-entity architecture for security and enforcement. The first two entities are the parent/guardian and the child. The parent/guardian (denoted as the "user") creates the privacy preference for the child (denoted as the "client") and in this way provides a form of verifiable parental consent as required by COPPA. The privacy preference implemented on the client's side is called the user privacy preference and the XML format file containing the preferences is called the user privacy preferences file (UPPF). The third entity is any merchant or website the client visits. The privacy policy of the merchant is specified in a merchant privacy policy and recorded in a

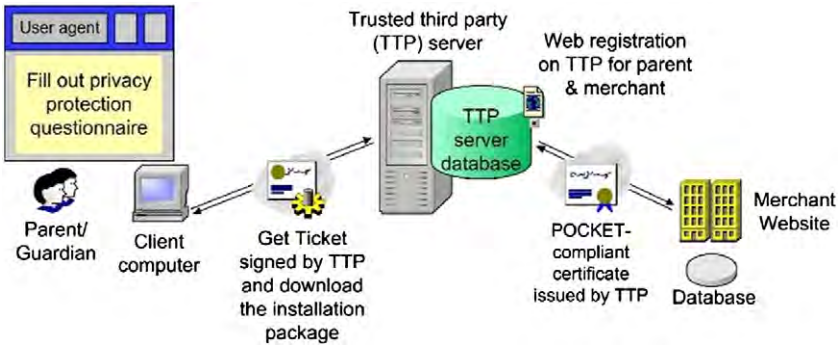


Fig. 1. POCKET registration phase.

pre-specified location as the merchant privacy policy file (MPPF). The trusted third party (TTP) forms the fourth entity involved in POCKET.

The use of a TTP is derived from the 3-entity architecture proposed for identity-based encryption (IBE) [31]. In POCKET, the role of a TTP is to provide mutual authentication—allowing the merchant and client to authenticate each other's policies (similar to trust seals), public key distribution and assignment of a (one time) TTP signed ticket to each client for access to POCKET compliant merchant websites. TTP also serves as an enforcement agency in case of disputes between the merchant and the client. We expect that use of the TTP will enhance trust in POCKET. This expectation is based on the idea of technological trust, that is defined as "an individual's willingness to be vulnerable to a technology based on expectations of technology predictability, reliability, and utility and influenced by an individual's predilection to trust technology [26]." Prior studies illustrate the importance that trust has in the overall adoption of an unfamiliar artifact [2,36,37].

We propose the extension of P3P specification by including additional tags required for compliance with COPPA. All the key elements of the P3P vocabulary will remain the same. However, additional categories to recognize the data collected from children will be added to the DATA-GROUP and DATA tags. For example, in addition to the user's (child's) financial information, it will also include financial information of parents. New categories will also include information regarding age-group, siblings, school or education institution, and so forth.

Websites provide hyper-text markup language (HTML) forms to collect the client's information. POCKET implements automatic information transfer and avoids forms completely. Some advantages of doing this in the context of protecting children's privacy are as follows: (1) it prevents the websites from collecting more information than specified in the policy. Forms may collect information that is optional and a child is not mature enough to know what information to disclose and what not to disclose, (2) the POCKET client (once validated) is guaranteed to provide only information that is absolutely necessary, and (3) the information package is transmitted securely to the website without the risk of being eavesdropped.

On the merchant's side, POCKET is implemented by adding a policy targeted towards children to their websites. This requires changes to the P3P policy file oriented towards the children visiting the website and the information collected from them.

3.2. Implementation of POCKET

The software implementation of POCKET consists of a user agent (UA) and browser helper object (BHO). Once installed on the client machine, the four entities exchange messages based on a protocol divided into three phases – registration, setup and transaction. The software installer package is available for download from the TTP server during the parent registration phase. The UA has two modes – parent-mode and child-mode. The software is setup on the client machine in the parent-mode. During setup, the UA provides a questionnaire to the parent. The parent's responses are converted to an UPPF and stored on the client machine. When the UA enters the child-mode it activates the BHO and enforces the preferences. The BHO coupled with the browser can intercept user communication with the Internet. For security purposes, the UA requires the parent's password for any modification of the privacy preferences and to switch back into parent-mode. The details of the phases in the POCKET framework are provided below.

Registration Phase – Fig. 1 shows the pictorial representation of the registration phase. The user performs a one-time registration accessing the TTP through a website. During this phase the user registers with the TTP server and creates an account. Although not particularly specified in the POCKET protocol, parental verification can be implemented at the time of registration. Parental verification is accomplished by a combination of online and offline mechanisms to ensure that only an adult can register as a parent. Because parental verification is only required once it is appropriate to demand a higher level of effort from the parent. The one time verification is possible because at account creation the parent creates a password that will be used for authentication at subsequent interactions. The TTP server assigns a unique ID to the user (parent/guardian). Registration provides the parent with the POCKET installer.

The merchant also registers with the TTP server in order to be POCKET compliant. The merchant provides answers to a questionnaire regarding the website's data collection practices and use policies. The answers to the questionnaire are converted into a machine readable XML format file and the MPPF is created. The merchant is required to deploy this file in a prescribed location on the merchant website. During the transaction phase, this file is compared with the UPPF. The TTP also provides the merchant with a POCKET compliant certificate during registration. The client uses this certificate to authenticate the merchant during transaction phase.

Setup Phase – The user configures the POCKET UA by executing an installer. The UA also requires the user to create a login and password (on the client machine). This login is only for the purpose of protecting POCKET's configuration on the client machine. The parent chooses the child's personal information that the merchant can collect. The user agent provides another dialog for the parent to enter the information. The client's information may include personal information (for example, full name, address and phone number), sibling data, school information among others. The parent can also configure the POCKET UA such that no information is collected from the child. The UA then converts the user's preference into a UPPF and stores it on the client's machine. The POCKET UA automatically enables the BHO after this configuration is complete. The BHO enforces the preferences specified in an UPPF.

Transaction Phase – Fig. 2 shows the interaction between the client and the merchant website during the transaction phase. When the client enters the merchant website's uniform resource locator (URL) in the browser, the BHO installed on the client's browser (without client involvement) requests the MPPF, the POCKET certificate and the merchant information collection practices. Here, we are assuming that the

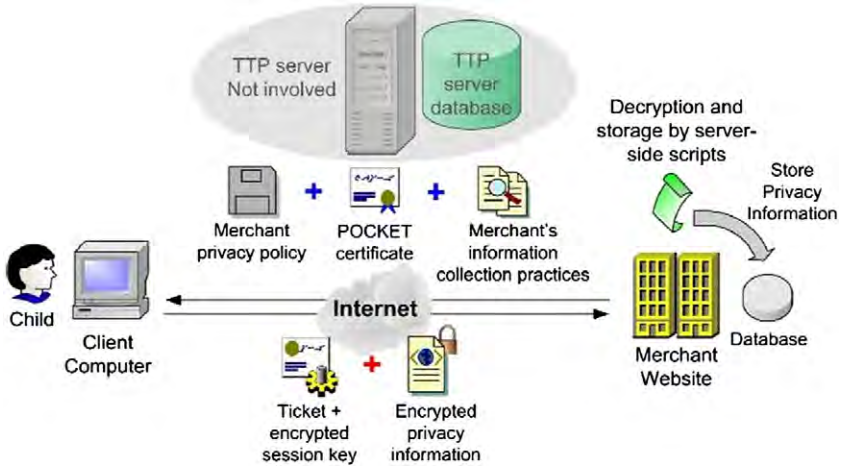


Fig. 2. POCKET transaction phase.

merchant complies with POCKET's requirements and places the MPPF in a pre-specified location. The POCKET agent decides to allow or block a website after comparing the MPPF and UPPF. If the policy and preferences do not match, the BHO displays a "privacy policies do not match" message to the client and blocks the website. If the MPPF and UPPF match, the client creates a merchant specific privacy information package (PIP). The PIP only includes the personal information requested by the merchant and is a subset of the information that the parent gave to be disclosed.

Using the proposed secure handshake protocol, the client side BHO uploads the PIP to the merchant site and allows the browser to display the website. The POCKET agent on the client machine creates a *log file* entry showing the transaction. The release version of the POCKET software will include uploading of a digital contract[1] along with the PIP. The log file and the digital contract are useful in enforcing merchant accountability.

3.2.1. Security features of the POCKET framework

The data exchange protocol, especially the transaction phase, between the client and the merchant website is vulnerable to several attacks. In this section, we analyze them and propose relevant countermeasures in the various phases of the client interaction with POCKET. Specifically, the transaction phase is vulnerable to unauthorized uploads and man-in-the-middle attacks.

With the POCKET system in place, merchant websites accept the client's PIP and store it for further processing. It is feasible for an anonymous user to upload spurious and harmful data to the merchant site, resulting in a Denial-of-Service (DoS) attack that prevents valid clients from accessing the website. This would happen if a person decided to send unrequested data repeatedly to the merchant site when the merchant site was expecting a PIP from the client. Without authenticating legitimate clients any data upload protocol fails to protect the merchant from attacks. As defined in the POCKET framework, the TTP implements a simplified Kerberos-like authentication mechanism [38] and provides mutual authentication between the client and the merchant. For mutual authentication, the TTP supplies a "certified ticket" for each client and a POCKET-compliant certificate to each merchant. The client's certified ticket prevents malicious users from uploading harmful data to the merchant website, while the POCKET-compliant certificate is verified (by the client) to determine merchant's POCKET-compliance.

The man-in-the-middle attack is another type of attack that can be launched against this system. This attack happens when a valid packet is intercepted and manipulated or processed for information. Potential problems with a man-in-the-middle attack are (1) eavesdropping on sensitive and personal information, (2) information modification, and (3) packet replay at a later time. In addition to mutual authentication, the TTP performs the role of a key distributor and employs a pretty good privacy (PGP) framework [38]. With public-key exchange between a client and a merchant, the confidentiality and non-repudiation of data can be provided by encryption with a session key and a digital signature, respectively. The replay packets can be identified and ignored by employing a typical challenge/response handshake protocol.

3.3. POCKET software prototype

We have completed a prototype of the POCKET UA and BHO for the Windows XP operating system. The current implementation of the BHO works for Microsoft's Internet Explorer version 6.0 (IE6) and can be easily extended for other versions and browsers. The POCKET artifact consists of a UA and BHO implemented in Visual C++. The UA is a simple dialog based application that is used to configure POCKET on the client machine. The parent configures POCKET with a setup password which protects the parent-mode from unauthorized access. After installation, the UA automatically presents the parent with the privacy preferences configuration dialog. This dialog box gives parents the option of what information they will allow merchants to collect from their child (See Fig. 3). The UA converts the parent's selections into an UPPF and stores it in the client's machine. In Fig. 3 the parent is setting up the permission for their child, Mike, allowing the collection of first name, age range, and zip code but not allowing any of the other information to be collected. At this point the parent can implement the choice that NO information be collected from the child by selecting none of the options. The UA provides the parent with a second dialog requesting the user to enter the actual information for the preference elements configured in Fig. 3. After configuration, the UA automatically enters the child-mode, starts the BHO and enforces this UPPF when the client visits any website. Fig. 4 shows the dialog for the UA once setup is complete and enabled on the client machine. Any shift from the child-mode to the parent-mode or closing of the UA needs the parent's setup password. Fig. 5 shows the dialog for the UA when POCKET has been disabled on the client machine.

We created mock merchant websites that support the MPPF required by the POCKET BHO. We tested the software implementation using these mocked websites. We used a simplified XML file format that is consistent with the P3P specifications to create the privacy preference files. We strongly feel that the POCKET framework is the best solution for enforcement of COPPA. It is an easy to use, automated

[1] A digital contract is a legal agreement between the client and the merchant regarding the collection and use of information gathered.

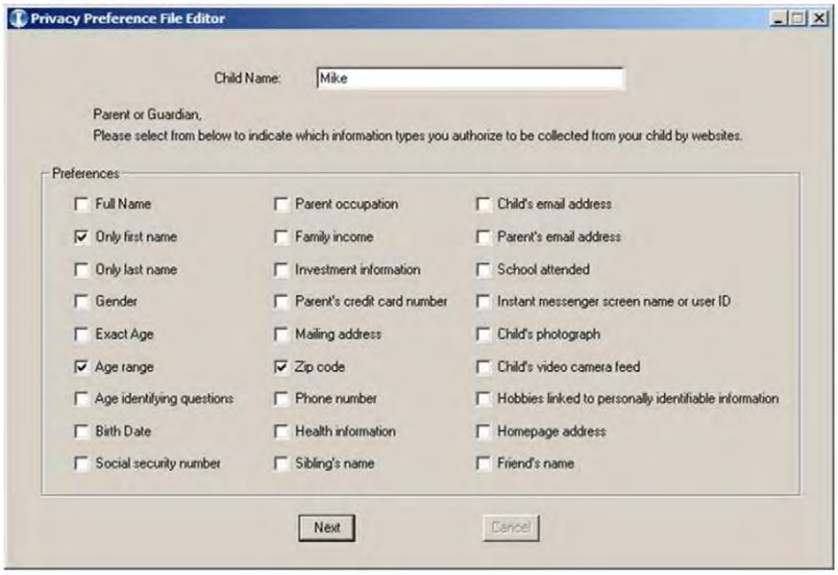


Fig. 3. Parent creating the UPPF for Mike.

tool that can be used by a technologically unsophisticated parent and deployed to protect children's privacy. It puts control into the hands of the parent and identifies the website visitor as a child. POCKET allows parents to implement the choice that NO information be collected from their children. Automation provides the advantage that the parents do not have to constantly supervise and worry about disclosure of personal information by their children. Once deployed, POCKET will provide a way to enforce the parental consent requirement of COPPA.

4. Evaluation of POCKET

An important aspect of the design of an IT artifact is the evaluation of the tool. In the context of POCKET, there are three different types of design principles that need to be evaluated for compliance:

1. The legal evaluation verifies if POCKET meets the legal requirements of COPPA.
2. The technical evaluation verifies if POCKET works as intended technically and is error free.
3. The behavioral evaluation verifies if POCKET meets the user requirements.

4.1. Legal evaluation

POCKET is designed to be a technical advancement of the requirements of COPPA, without displacing or becoming a safe harbor program. In essence, it will strengthen the protection of children by offering a more robust method for implementing COPPA and subsequent FTC regulatory requirements. Therefore, it is not expected that every design principle will be met; in the charts below the italicized elements refer to future and safe harbor elements necessary to meet all of the regulatory requirements. As can be seen from Table 4, POCKET is designed to strengthen the legal requirement of parental consent, and it also includes important methods for subsequent changes to consent and overall parental control.

The purpose of designing POCKET based on a number of design principles was to ensure that it was driven by the overarching kernel theories identified prior to its development. The resulting evaluation, provided above, demonstrates that POCKET successfully achieved the legal specifications as mandated by COPPA.

4.2. Technical evaluation

The technical evaluation of POCKET included several steps. First, there was in-depth software testing. The main goal of testing the POCKET software is to ensure that the system works in the specified manner when a certain set of inputs are given. Further, the system must not give unexpected results thereby undermining its dependability. POCKET is targeted at parents who must trust that the system can allow/block websites based on the given preferences. In order to make sure that this is true, we tested the system extensively. The testing procedure consisted of two stages: black box and white box testing, which are described in detail in Appendices A and C.

Black box testing involves the selection of different inputs at the user interface. It allows the tester to concentrate on hard-to-reach paths in other forms of testing and also helps to assure a high degree of reliability in the operation of the entire system. For POCKET, we

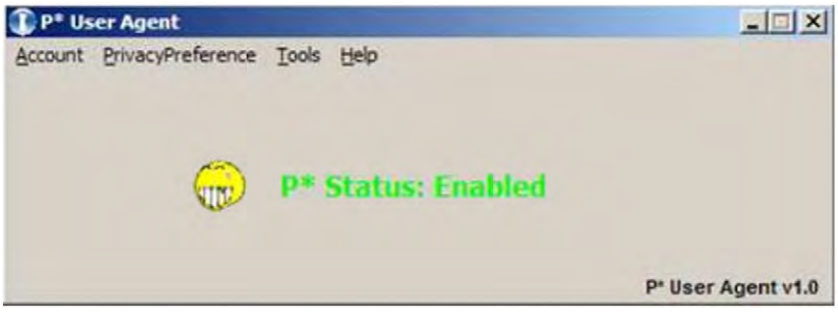


Fig. 4. Status enabled dialogue for the POCKET user agent.

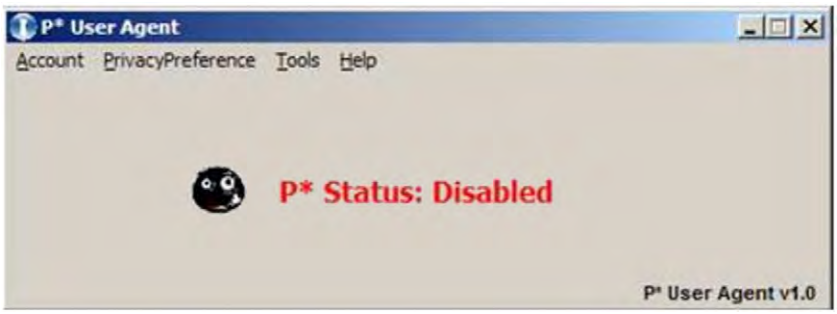


Fig. 5. Status disabled dialogue for the POCKET user agent.

tested the user interface (UA) and the machine executable (BHO) components. For black box testing, we identified all possible paths in the software. There were a total of 283,545,222,346 paths covered by black box testing, and the results translated to 99.87% path coverage. One software bug was identified during black box testing and fixed.

White box testing involves testing POCKET with knowledge of the inner workings of the software and is used for hard-to-test paths such as paths constrained by some inputs to the function or un-testable (see Appendix C for examples). We analyzed the remaining 373,293,146 paths and found 10 paths to be untestable because they were the result of two 'if' statements. The condition of one 'if' statement was the 'else' condition of another 'if' statement, making them practically impossible to be in the same path, though theoretically possible. Seventeen paths were found to be redundant due to the coding style. They were fixed in the code.

In summary, since 100% statement coverage and 100% path coverage are considered adequate enough to deem the system tested, POCKET is considered to be extensively and adequately tested.

The second phase of technical evaluation testing was to verify that the technical design principles were met. Table 5 shows how each of the proposed design principles were evaluated and the results.

In summary, the POCKET prototype leverages existing tools and concepts from the kernel theories presented in Section 2.2, and meets the requirements established previously established. Several of the design principles derived from these kernel theories and the technical environment were also tested in the behavioral (user) evaluation, such as ease of use and ease of navigation.

4.3. User/design evaluation

The design of POCKET involves three sets of stakeholders: parents, merchant website owner, and a trusted third party. The user evaluation of POCKET, however, targets only the merchant website and the parents since they are the only players involved in the transaction phase of POCKET. The role of the trusted third party is to hold certificates for the verification of the merchant website, similar to VeriSign™'s role as a security certificate provider.

To evaluate POCKET from a parent's perspective, we conducted an online survey of parents with children under the age of 13. First, after answering general demographic questions, parents viewed a demonstration of the POCKET software prototype. We then asked them questions to ensure the design of POCKET met the specifications that parents gave us during the focus group stage of the research. In particular we focused on measuring ease of use [41], perceived behavioral control [39], and the perceived cost-benefit of POCKET. We further measured the impact that social norms [41] has on adoption as it was a factor that emerged from our focus groups but was not a behavioral component that could be controlled for in the design of POCKET.

Evaluators were recruited using a convenience sample of parents of children below the age of 13 in different regions of the United States. Authors contacted parents not knowledgeable about the research and provided them with a link to the survey. To encourage participation, small prizes were offered in a drawing among participants. The solicitation email also requested that parents forward the link to the survey to other parents they knew who had children under the age of 13.

For validation purposes, and given the few items our instrument included, we targeted 25 user responses. We received 19 responses and after those with missing data were removed, we had 15 data points to evaluate behavioral requirements compliance. The respondents were on average 42.8 years old. 87% were Caucasian and 60% were males. Respondents indicated that the average time online for their children (below the age of 13) was 4.3 h per week.

Before evaluating the behavioral requirements responses, we tested the reliability and validity of the instruments used. All constructs with more than one item had Cronbach's alphas greater than 0.70, suggesting reliable measures. Construct validity was tested using a confirmatory factor analysis, with no item loading issues. For the evaluation of the POCKET artifact, our goal was to ensure the tool met the predefined requirements that emerged from the focus groups. As such, an average of each measure was calculated except for cost-benefit, which used a

Table 4
Legal evaluation of POCKET.

Design principles	Evaluation evidence
POCKET should provide a way to verify the privacy practices of websites.	POCKET compares the privacy preference file with the privacy policy of the website.
POCKET should automate the process of parents providing their consent to the release and use of their children's information at a granular level as it matches the parent's predefined set of preferences.	As seen in Fig. 3 and discussed in Section 3.2, during the *Setup Phase*, parents choose whether information can be released, and if so what type of information. As seen in Fig. 2, parent choices must match with what websites will collect in order for children to successfully share information with a given website.
POCKET should provide a method for parents to review information that has been provided to websites and notify websites if the information should be deleted.	As seen in Fig. 2 and discussed in Section 3.2, POCKET creates a *log file* entry showing the transaction. Further, a digital contract is created and sent along with the personal information to the website. The log file and the digital contract can then be utilized to enforce merchant accountability to parental requests.
POCKET should properly secure information that it contains, as well as provide accurate information to website merchants it shares information with on the parent's behalf.	As discussed in Section 3.2.1, POCKET was designed with a number of measures to ensure the secure transfer and storage of information. Further, to ensure accuracy POCKET was built using an expansion of P3P, which includes accurately tagging the information sent to merchant websites.

Table 5
Technical evaluation.

Design principles	Evaluation evidence
POCKET should be easily downloadable once parents are registered.	Black box testing
POCKET should be easy to install using a self-extractor file.	Black box testing
The User Interface should be graphical and easy to navigate with a combination of menu items, dialog boxes, and easy to interpret error messages.	Design as exemplified in per Figs. 3–5
POCKET should be developed initially for Internet Explorer using the Browser Helper Object (BHO) tool.	Design as per section 3.2
The transaction phase (whether the transfer of information is approved or not) should be transparent to parents once POCKET is installed and working.	Black box testing
POCKET requires secured transmissions of information between the parents, website, and trusted third party machines.	Design as per section 3.2.1 and black box testing
POCKET should automatically compare the Privacy Preference File from POCKET with the website's privacy practices file using P3P User Agent concepts.	Design as per section 3.2 and 3.3, and black box testing
POCKET should allow parents to modify settings as desired.	Design as per section 3.2 and 3.3, exemplified in Fig. 3, and black box testing
POCKET should include four phases: registration, installation, transaction, and post-transaction phases.	Design as per section 3.1 and 3.2

single item. Items were measured on a Likert-like scales ranging from 1 to 7. As can be seen from Fig. 6, evaluation results of all measures that can be controlled through the development of POCKET (ease of use, perceived behavioral control, and cost benefit) indicate that parents believe POCKET meets their expectations, which suggests we were successful in developing a tool that meets the needs expressed by parents prior to the design of POCKET. The social norm construct, which cannot be controlled within the development of POCKET, is also rated above the midpoint of the scale, indicating that while not the most important factor in determining parents' potential use of POCKET, what other parents do will also be important for determining parents' use of POCKET.

As can be seen from Table 6, POCKET successfully met the behavioral design requirements as specified in Section 2.3.3.

The design of POCKET was further validated with web merchants, through interviews with two website owners. One of them owns an online retail website while the other owns a sport services website. Neither of the owners knew of the legal requirements of COPPA, although both could be subjected to those requirements. Both owners indicated that they liked the concept of POCKET and the resulting artifact, and would use POCKET if it assured them of COPPA compliance. However, they also indicated that they would not use it unless a critical mass of parents was using the POCKET software as well. This creates a chicken and the egg problem because parents also say that they would use POCKET if other parents would use it.

5. Discussion

POCKET is a prototype designed to meet the legal requirements of COPPA and give parents a tool to protect their children's online privacy. In designing POCKET, we followed the design science principles presented by Hevner and his colleagues [19], who suggest that IS research is at "the confluence of people, organizations, and technology (p. 77)." Design research is an important area in the field of information systems. Orlikowski and Iacono [35] describe five meta-categories that

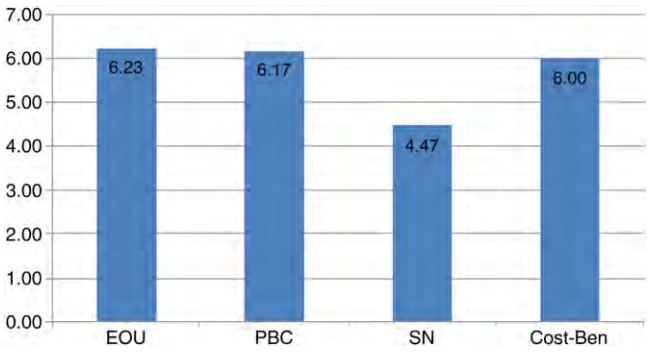


Fig. 6. Comparison of means for behavioral evaluation measures.

conceptualize design research: the tool view, the proxy view, the ensemble view, the computational view, and the nominal view. The tool view is described as focusing on the description of the "technical features of a new technology to understand what that technology will do" (p123). Orlikowski and Iacono argue that this approach limits IS research to more of a black box approach and suggest that IS researchers should instead strive towards presenting more powerful conceptualizations of how IT can be used within organizations. Indeed, one common issue for social scientists is that they often present artifacts as black boxes [35]. The proxy view focuses on "one or a few key elements in common that are understood to represent or stand for the essential aspect, property, or value of the information technology." The computational view "concentrates expressly on the computational power of information technology." This type of design research focuses on the "capabilities of the technology to represent, manipulate, store, retrieve, and transmit information, thereby supporting, processing, modeling, or simulating aspects of the world." The nominal view of technology considers technology as absent, indicating that "the technology is invoked in name only, but not in fact." Finally, the ensemble view of technology requires that researchers describe how the components of the designed artifact can be applied to a socio-economic activity [35], focusing on the interaction of the technology used, the people involved in the design process, as well as the target audience of the finished product.

In this research, we took the challenge presented by Orlikowski and Iacono by explaining how the design of POCKET was informed by three disciplines and their interaction, and showing how POCKET is tested by the design team, as well as the intended target audience. This clearly represents the ensemble view. More specifically, we combine the view of technology as a development project when we describe the process of developing POCKET and the technology as an embedded system when we conceptualize POCKET as an evolving system embedded in a complex and dynamic context exemplified by the legal and behavioral requirements identified in its development. Interestingly, Orlikowski and Iacono [35] find that the ensemble view was the least represented category in their review of articles in the *Information Systems Research* journal. Their recommendation for using the ensemble view, "which [does] engage with the social and embedded aspects of technology development and use" (p. 132) includes making sure to consider the conditions, both material and cultural, that bind the IT artifacts, and to consider their dynamic nature. The development of POCKET follows these recommendations and adds to the limited literature that explicitly considers the IT artifact.

In addition to answering the call for more research that explicitly considers the IT artifact embedded in its social technical context [35], the research shows how the guidelines proposed by Hevner and his colleagues [19] allow design science researchers to lift the lid on the "black box" of their artifacts. How we followed the seven guidelines is presented in Table 7. In summary, the contributions of this study fit in the design and action theoretical contributions as discussed in

Table 6
Behavioral evaluation of POCKET.

Design principles	Evaluation evidence
POCKET should be easy to use.	As illustrated in Fig. 6, a review of POCKET by parents showed that they believe it is easy to use.
POCKET should meet legal requirements.	As demonstrated in the Legal Evaluation in Section 4.1, POCKET meets the legal requirements.
POCKET should create log files, to be utilized at the parent's discretion.	As demonstrated in the Legal Evaluation in Section 4.1, POCKET creates log files. In addition, as presented in Section 3.2 and 3.3, the design of POCKET includes a parent-mode and a child-mode. One of the advantages of parent-mode is that it turns off the POCKET protection as well as the logging capabilities.
POCKET should provide increased control over information released by children.	As illustrated in Fig. 6, a review of POCKET by parents showed that they believe it increases their control.
POCKET should provide maximum value at a minimal cost.	As discussed in section 3.2, POCKET is downloadable to parents. Further, as illustrated in Fig. 6, POCKET is evaluated by parents as ranking high on the cost-benefit perception.

Gregor [18]. An artifact was designed following established design science guidelines. As a result, our contributions are incremental to prior work on information privacy in general, privacy-enhancing tools (PETs), and design science research. In addition, from a research standpoint, the study demonstrates the value of the focus group research approach as called for by Bélanger [3].

5.1. Future research directions

The development and testing of the POCKET artifact is a first small step in the direction of enforcing the protection of children's privacy online. In this section, we briefly discuss some additional ideas for future research.

First, as research utilizing the approach set forth by POCKET continues, it should consider moving into the protection of children's privacy in a mobile computing setting. Mobile apps designed for use by children do not clearly state in their privacy policy how the apps collect data or interact with social networking sites [17]. However, the FTC does enforce COPPA in the mobile computing sector [16], but is pushing for extensions to what COPPA covers to explicitly include mobile apps as well as expand the definition of "personal information" to include such things as device identifiers, geo-location information, and IP addresses [15]. Such enforcement of and changes to COPPA signify that there is a growing need for software such as POCKET in the mobile computing environment as well as in the PC environment as designed. As future iterations of POCKET are made, focus should be turned towards expanding the coverage of POCKET to additional personally identifiable information such as location, personal information in mobile cookies, and device identifiers. Control will be returned to parents by giving them the ability to specify, at a granular level, the information their children can share while using mobile apps. Without some form of technological enforcement there is no guarantee that mobile apps are not collecting this information. POCKET was specifically developed to address the legal requirements of COPPA, in addition to the technical and behavioral requirements identified. However, there are other legal frameworks regarding financial and health information online. There are also different legal frameworks for different countries around the world. One potential avenue for future research would therefore be to adapt POCKET to these different legal frameworks.

5.2. Limitations

One of the limitations in this research, as in most design science research [1,9,33,34,43], is that continued use could not be evaluated. Kim and Malhotra [35] suggest that continued use might be a more important measure for the evaluation of artifacts than intentions to use. This is consistent with a discussion of post-adoptive behaviors [21] in which it is highlighted that even though organizations have invested in a wide variety of information systems, many of these software are underutilized by their potential users. However, this would require that a critical mass of parents and a critical mass of web merchants decide to use POCKET and that it is incorporated in web browsers such as Internet Explorer by the developers of such browsers. Since most merchants prefer not to limit their data collection, it is likely that this would only occur in the case of mandated use by a government agency.

6. Conclusion

In this paper, we have presented a new privacy-enhancing artifact called POCKET, which has been designed as a prototype for protecting children's privacy online. POCKET implements an automatic way to obtain verifiable parental consent as required by COPPA. It is an easy-to-use tool that technologically unsophisticated parents can deploy to protect their children's privacy. With POCKET, parents can control the

Table 7
Design science guidelines and POCKET [19]*.

Design science guideline	POCKET compliance
Problem relevance (2)	POCKET addresses the need for technology to enforce COPPA, a law that seeks to protect the privacy of children online.
Design as a search process (6)	The design of POCKET followed rigorous search, design and testing processes. In developing POCKET, laws were extensively reviewed to ensure POCKET met the legal requirements of COPPA. Focus groups were conducted to ensure that the resulting artifact would meet parents' usage requirements. Existing technologies were evaluated to ensure that best practices were incorporated in POCKET. The design process involved building alpha and beta versions of the artifact with appropriate modifications as necessary (see appendix B). Testing then included white box and black box testing (see appendix C).
Design as an artifact (1)	The result of this research is the POCKET artifact.
Design evaluation (3)	The evaluation of POCKET included legal, technical, and behavioral evaluations.
Research rigor (5)	The development of POCKET followed design methodologies proven in the design science literature. Evaluation of POCKET likewise included a rigorous evaluation process.
Research contributions (4)	POCKET is an implementation of an artifact that is an extension of P3P, which provides mechanisms for accountability and enforcement of COPPA.
Communication of research (7)	In this paper, we have presented this artifact with sections intended for a management oriented audience, as well as sections intended to communicate the design to a technical audience. Several conference papers were also presented during and after the project completion (references withheld).

* We modified the order of the guidelines to match the order we present them in this paper.

personal information collected by websites from their children without constantly monitoring their activities online. The client's preferences and the merchant policy files have a format that is consistent with the P3P specifications. POCKET assumes the merchant policy file is placed in a specified location on the server, and POCKET includes a secure protocol for uploading personal information from the client to the merchant. It also establishes mechanisms for merchant accountability by maintaining activity logs. With mock merchant websites, the prototype demonstrated its promise in offering a COPPA-compliant platform. The evaluation performed demonstrates that this tool is free from bugs and meets the needs of parents in protecting their children's privacy online.

This research provides contributions for researchers and the general public alike. From a research perspective, POCKET illustrates how existing technology such as P3P can be leveraged to provide a working solution to communicate information about third parties. It also illustrates how focus groups can be relied upon to inform the development of a software tool. The POCKET project shows that design is as much an activity as it is the end product. POCKET results in important design research contributions since it adds to the knowledge base in computer engineering, information systems and business law. It provides "contributions to the archival knowledge base of foundations and methodologies [19] (p81)." By communicating what was discovered during the development of POCKET future researchers can inform their research as well as expand on what was done on this project. From the general public's perspective, this research provides an actual tool, which when fully implemented could provide an added layer of protection for parents to rely upon in protecting their children's privacy online. The use of focus groups along with the evaluation of the finished product illustrates that this tool meets the requirements parents expressed.

Appendices A, B, and C. Supplementary data

Supplementary data to this article can be found online at http://dx.doi.org/10.1016/j.dss.2012.11.010.

References

[1] M.D. Ahmed, D. Sundaram, Sustainability modelling and reporting: from roadmap to implementation, Decision Support Systems 53 (3) (2012) 611–624.
[2] S. Ba, P.A. Pavlou, Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior, MIS Quarterly 26 (3) (2002) 243–268.
[3] F. Bélanger, Information systems theorizing using focus groups, Australasian Journal of Information Systems 17 (2) (2012) 109–135.
[4] 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.
[5] L.F. Cranor, P3P: making privacy policies more useful, IEEE Security & Privacy Magazine 1 (6) (2003) 50–55.
[6] 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, AT&T Labs-Research, 2003.
[7] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. Reagle, M. Schunter, D.A. Stampley, R. Wenning, The platform for privacy preferences 1.1 (P3P1.1) specification, http://www.w3.org/TR/P3P11/2006 (Last Accessed 12 September 2007).
[8] L.F. Cranor, P. Guduru, M. Arjula, User interfaces for privacy agents, ACM Transactions on Computer-Human Interaction (TOCHI) 13 (2) (2006) 135–178.
[9] O.F. El-Gayar, B.D. Fritz, A web-based multi-perspective decision support system for information security planning, Decision Support Systems 50 (1) (2010) 43–54.
[10] EPIC, EPIC public opinion and privacy page, http://www.epic.org/privacy/survey/default.html 2007 (Last Accessed 11 September 2007).
[11] EPIC, Junkbusters, Pretty poor privacy: an assessment of P3P and internet privacy, http://www.epic.org/reports/prettypoorprivacy.html 2007 (Last Accessed 12 September 2007).
[12] FTC, FTC seeks comment on proposed COPPA rule amendment, http://www.ftc.gov/opa/2005/01/coppafrn.htm 2005 (Last Accessed 12 September 2007).
[13] FTC, Xanga.Com to pay $1 million for violating children's online privacy protection rule, http://ftc.gov/opa/2006/09/xanga.htm 2006 (Last Accessed 12 September 2007).
[14] FTC, COPPA protects children but challenges lie ahead, http://www.ftc.gov/opa/2007/02/copparpt.shtm 2007 (Last Accessed 13 November 2007).
[15] FTC, Children's online privacy protection rule, Federal Register 76 (187) (2011) 59804–59833.
[16] FTC, Mobile apps developer settles FTC charges it violated children's privacy rule, http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm 2011 (Last Accessed 16 March 2011).
[17] FTC, Mobile apps for kids: currect privacy disclosures are disappointing, http://ftc.gov/os/2012/02/120216mobile_apps_kids.pdf 2012(Last Accessed 19 March 2011).
[18] S. Gregor, The nature of theory in information systems, MIS Quarterly 30 (3) (2006) 611–642.
[19] A.R. Hevner, S.T. March, J. Park, S. Ram, Design science in information systems research, MIS Quarterly 28 (1) (2004) 75–105.
[20] J.S. Hiller, F. Belanger, M. Hsiao, J.M. Park, Pocket protection, American Business Law Journal 45 (3) (2008) 417–453.
[21] J. Jasperson, P. Carter, R. Zmud, A comprehensive conceptualization of post-adoptive behaviors associated with information technology enabled work systems, MIS Quarterly 29 (3) (2005) 525–557.
[22] D.M. Kristol, HTTP cookies: standards, privacy, and politics, ACM Transactions on Internet Technology 1 (2) (2001) 151–198.
[23] R.A. Krueger, Focus groups: a practical guide for applied research, 2 ed. SAGE Publications, Inc., Thousand Oaks, CA, 1994.
[24] W. Kuechler, V. Vaishnavi, A framework for theory development in design science research: multiple perspectives, Journal of the Association for Information Systems 13 (6) (2012) 395–423.
[25] O. Kwon, A pervasive P3P-based negotiation mechanism for privacy-aware pervasive e-commerce, Decision Support Systems 50 (1) (2010) 213–221.
[26] S.K. Lippert, Investigating postadoption utilization: an examination into the role of interorganizational and technology trust, IEEE Transactions on Engineering Management 54 (3) (2007) 468–483.
[27] S.T. March, G.F. Smith, Design and natural science research on information technology, Decision Support Systems 15 (4) (1995) 251–266.
[28] Microsoft, Internet explorer 7.0 features in windows vista: parental controls, http://www.microsoft.com/windows/products/windowsvista/features/details/parentalcontrols.mspx (Last Accessed 12 September 2007).
[29] Microsoft, Microsoft internet explorer privacy statement, http://www.microsoft.com/windows/ie/ie7/privacy/ieprivacy_7.mspx (Last Accessed 29 October 2007).
[30] M.B. Miles, A.M. Huberman, Qualitative data analysis: an expanded sourcebook, Sage Publications, Thousand Oaks, CA, 1994.
[31] M.C. Mont, P. Bramhall, Ibe applied to privacy and identity management trusted, in: Technical Report, HP Laboratories, Bristol, 2003.
[32] M.C. Mont, S. Pearson, P. Bramhall, Towards accountable management of identity and privacy: sticky policies and enforceable tracing services, in: 14th International Workshop on Database and Expert Systems Applications, 2003, pp. 377–382.
[33] J. Muntermann, Towards ubiquitous information supply for individual investors: a decision support system design, Decision Support Systems 47 (2) (2009) 82–92.
[34] E.W.T. Ngai, T.K.P. Leung, Y.H. Wong, M.C.M. Lee, P.Y.F. Chai, Y.S. Choi, Design and development of a context-aware decision support system for real-time accident handling in logistics, Decision Support Systems 52 (4) (2012) 816–827.
[35] W.J. Orlikowski, C.S. Iacono, Research commentary: desperately seeking "IT" in IT research—a call to theorizing the IT artifact, Information Systems Research 12 (2) (2001) 121–134.
[36] P. Ratnasingam, The importance of technology trust in web services security, Information Management & Computer Security 10 (5) (2002) 255–260.
[37] P. Ratnasingam, D. Gefen, P.A. Pavlou, The role of facilitating conditions and institutional trust in electronic marketplaces, Journal of Electronic Commerce in Organizations 3 (3) (2005) 69–82.
[38] W. Stallings, Cryptography and network security, principles and practices, 3rd ed. Pearson Education Inc., 2003.
[39] S. Taylor, P.A. Todd, Understanding information technology usage: a test of competing models, Information Systems Research 6 (2) (1995) 144–176.
[40] R. Turn, W.H. Ware, Privacy and security issues in information systems, IEEE Transactions on Computers C-25 (12) (1976) 1353–1361.
[41] V. Venkatesh, M. Morris, G. Davis, F. Davis, User acceptance of information technology: toward a unified view, MIS Quarterly 27 (3) (2003) 425–478.
[42] W3C, Extensible markup language (XML) 1.1, http://www.w3.org/TR/xml11 2006 (Last Accessed 12 September 2007).
[43] H. Xu, R.E. Crossler, F. Bélanger, A value sensitive design investigation of privacy enhancing tools in web browsers, Decision Support Systems 54 (1) (2012) 424–433.

France Bélanger is Professor and Tom & Daisy Byrd Senior Faculty Fellow in the Department of Accounting and Information Systems at Virginia Tech. Her research focuses on the impacts of communication technologies on individuals and organizations, in particular for distributed work and e-business, and on information privacy and security. She is widely published in the information systems field, including in such journals as Information Systems Research, MIS Quarterly, Communications of the ACM, Journal of Strategic Information Systems, various IEEE Transactions, Information Systems Journal, and many others. Dr. Bélanger co-authored the books E-Business Technologies (2003), and Evaluation and Implementation of Distance Learning: Technologies, Tools and Techniques (2000). She is Associate Editor of MIS Quarterly. Her work has been funded by several agencies, corporations and research centers, including the National Science Foundation. She held a Fulbright Distinguished Chair in MIS in 2006.

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, the Journal of Information Systems Security, Americas Conference on Information Systems, and Hawaii International Conference on System Sciences. He also serves on the editorial review board for the Journal of Organizational and End User Computing and the Journal of Information Systems Security. Prior to his academic career he worked as a database programmer, where he led many projects to completion and coordinated the work of others.

Janine S. Hiller is a Professor of Business Law at Virginia Tech. Dr. Hiller's research focuses on the challenges and policy issues of how traditional law and legal institutions can sufficiently address and accommodate the evolution of the advanced technological environment. Electronic commerce makes her research more complex, since it is international in nature, and therefore, international principles and norms must be considered. Research in electronic commerce and the law has included various aspects of relationships between electronic commerce and privacy, security and trust, and electronic government and privacy. Her research articles have appeared in American Business Law Journal, Banking Law Journal and Real Estate Law Journal.

Dr. Jung-Min "Jerry" Park received his Bachelor's degree and Master's degree both in Electronic Engineering from Yonsei University, Seoul, Republic of Korea, in 1995 and 1997, respectively. From 1997 to 1998, he was a cellular systems engineer at Motorola Korea, Inc. Dr. Park received the PhD degree in the School of Electrical and Computer Engineering at Purdue University in 2003. In the fall of 2003, he joined the faculty of the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University (Virginia Tech) as an assistant professor. Dr. Park is a recipient of a 2008 NSF CAREER Award and a 1998 AT&T Leadership Award. He is a member of the IEEE and ACM.

Michael S. Hsiao is currently a Professor in The Bradley Department of Electrical and Computer Engineering at Virginia Tech. He is a recipient of the National Science Foundation Faculty Early Career Development (CAREER) Award. His current research interests include architectural-level and gate-level automatic test pattern generation (ATPG), design verification and diagnosis, fault simulation and defect coverage evaluation, design for testability (DFT), test set compaction, power estimation and management in VLSI, computer architecture, parallelization, and reliability.

Research in Progress: The Privacy Helper ©2013: A Tool for Mobile Privacy

Workshop for Information Technology and Systems (WITS) 2013

France Bélanger and Robert E. Crossler

INTRODUCTION

Information privacy refers to an individual's ability to control information about themselves (Bélanger and Crossler 2011; Bélanger et al. 2002). In today's society, concerns about information privacy in the online environment have been growing for all individuals, but even more so for individuals able to use technology but unaware of the potential privacy pitfalls of the digital society. Exacerbating the problem of online privacy is the rapidly changing technological environment provided by mobile devices that allow easy tracking of users and increased sharing of information. In fact, the FTC and state of California recently began enacting laws enforcing privacy protection on mobile devices (Ahearn 2012 ; FTC 2011). Although there is an increased interest in research on location-based services (Bélanger and Crossler 2011), most users remain unaware of the privacy settings on their mobile devices, and once made aware of such settings, they desire to remove the location tracking settings that are set by default (Sadeh and Kelly 2011). Furthermore, the use of "apps" in mobile devices provide opportunities for individuals to create information gathering tools hidden from users who download these apps (McCarthy 2009). One example being implemented by companies is apps for direct mobile marketing, either through subscription or proximity (e.g., Reichhart et al. 2013; Shang et al. 2009; Sneps-Sneppe and Namiot 2013). This approach gives companies the ability to perform target marketing to smartphone users when they are near a given location, such as a business within a shopping mall. Further assisting companies in their ability to market directly to mobile devices is the use of Bluetooth Low Energy technologies. This technology was released with iOS7 and updates to the Android operating system. In iOS7, this is referred to as iBeacon and allows marketers to know the exact location of users

within stores (Epstein 2013; Gottipati 2013). As the risks of information gathering apps and location-based services tracking increases and users continue to remain unaware of these risks, a potential information privacy black hole exists. It is this issue that the present research seeks to address.

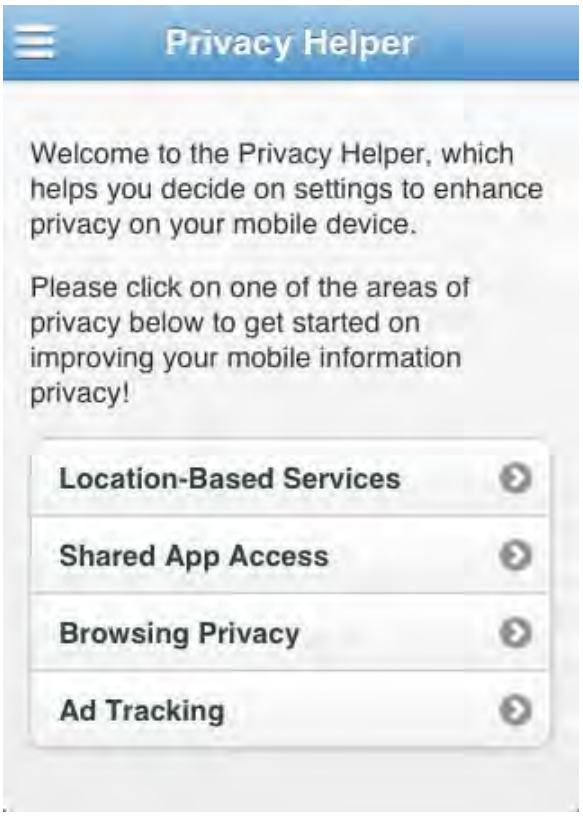
In this paper, we draw on the recommendations of Hevner et al. (2004) and the calls for design science artifacts in privacy research (Bélanger and Crossler 2011; Xu and Bélanger 2013) to develop a smartphone application for privacy education and training entitled The Privacy Helper©2013. The Privacy Helper will help users increase their privacy when using their mobile devices. In doing so, we draw on various theories to inform our design and to evaluate Privacy Helper's effectiveness (Kuechler and Vaishnavi 2012). The following section provides a description of Privacy Helper. The proposed method of evaluating this application is then presented.

Privacy Helper © 2013

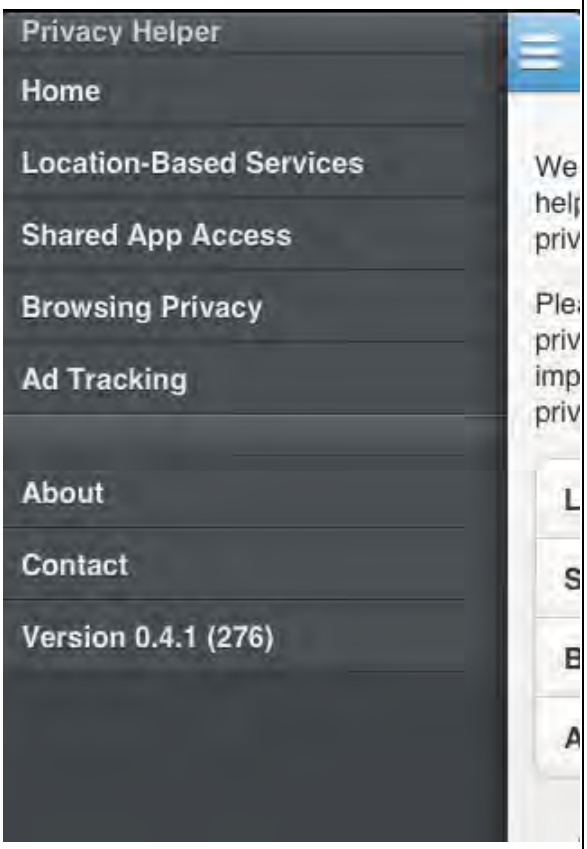
The design of Privacy Helper © 2013 was an iterative process so the development of the app could include modifications to the proposed design principles based on user feedback. The target application to demonstrate this proof of concept is an application that enables users of iPhones to be guided through the various privacy settings within the device so that they can adjust their settings accordingly. The resulting application provides smartphone users with a friendly guide to assist them in aligning their smartphone settings with what their information privacy views are. This guide is available to users in both a menu-based text only format to tell them what to do and in a voice format that plays step-by-step instructions while guiding them through the process of changing privacy settings.

Privacy Helper © 2013, as seen in Figure 1 Panel A, was designed using a model-view-controller paradigm (Krasner and Pope 1988). Due to the simplicity of the design and the user interface, the particular focus was on the view and controller perspectives of the paradigm. Views provided the ability to utilize web HTML and CSS code to display information. Controllers were utilized to navigate

users through various events as they click various links in the application. The controllers would then pass data to the various views that were created. This approach allowed for a modular design of the application and for various components to be modified without affecting other components. One of the controls utilized was that of using various 'drawers', as seen in Figure 1 Panel B. This allowed for a standardized menu to be provided to the user from anywhere within the app.



Panel A: Privacy Helper Main Screen

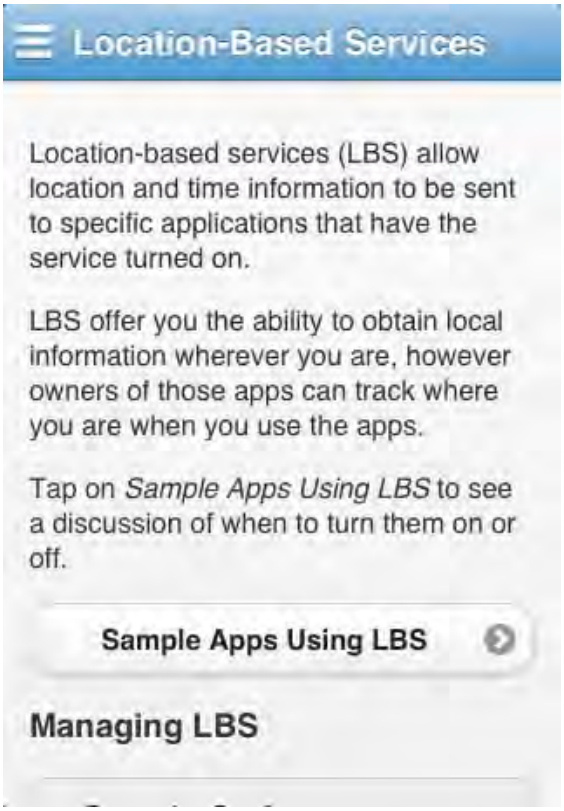


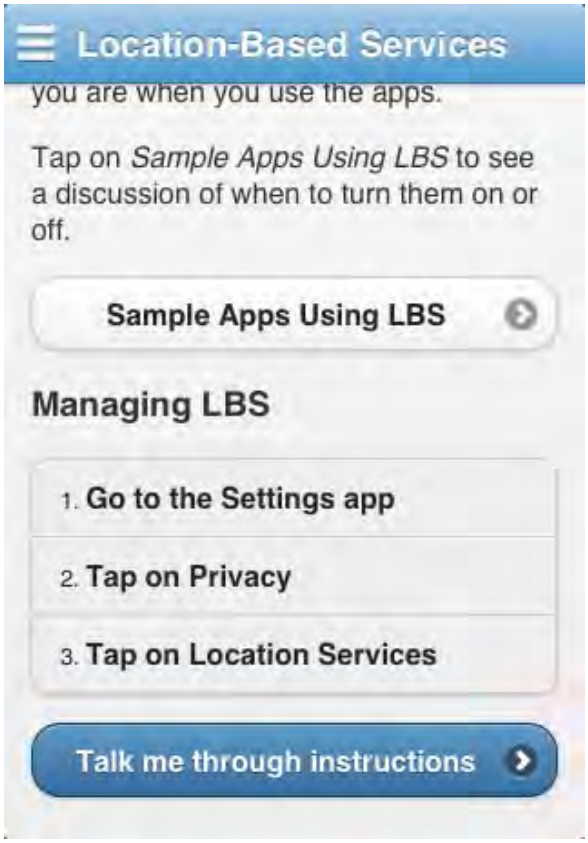
Panel B: Privacy Helper Left 'Drawer'

Figure 1: Views of Privacy Helper © 2013

Navigation through Privacy Helper © 2013 was designed to be as intuitive and user friendly as possible. Upon entering the main screen, all one has to do to move through the app is select one of the privacy areas they would like more information about. Once they have done, then they are taken to another screen, as displayed in Figure 2 Panel A. A description of what each privacy area is concerned

with is provided within each of the areas. In the example provided, based on location-based services a further option is provided to describe how various applications utilize location-based services. If the user scrolls down on this screen, he is provided with directions on how to adjust his location-based services, as seen in Figure 2 Panel B. They are also provided with the ability to have an audio tour that will talk them through how to do this while they are evaluating their current settings. This was designed so users would not have to remember what to do, but instead be told what to do while they were making decisions. Such an approach was necessary as the iOS ecosystem does not allow for apps to make system level changes. A similar design was created for each of the privacy settings that users can control in iOS6.





Panel A: Location-Based Services Screen	Panel B: Location-Based Services Directions

Figure 2: Views of Privacy Helper © 2013 Location Based Services Functionality

Evaluation

Evaluation of Privacy Helper © 2013 is a two-step process. First users will be presented with an opportunity to use Privacy Helper © 2013. After using the app, they will be asked a series of questions to determine whether the app meets the design principles as identified prior to its creation. After any iterative modifications are made as a result of this evaluation, a second round of evaluation will occur. This will be done to test the effectiveness of the app at improving privacy protection practices. To evaluation this portion of Privacy Helper © 2013's effectiveness, an experiment will be conducted. This experiment will provide two different levels of training – one by using the app and another by providing the same information in a static webpage. Participants in the experiment will report on their application setting prior to the experiment. This will be followed up by the treatment they are to receive. After completing the training, the devices will be examined again for various settings. A control group will also be utilized to ensure that the report of settings did not overly influence changes in the experimental manipulations.

References

Ahearn, T. 2012 "Mobile App Developers Must Comply with California Online Privacy Protection Act by November 29," *ESR News*), November 28.

Bélanger, F., and Crossler, R.E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp 1017-1041.

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

Epstein, Z. 2013. "The dark side of Apple's iBeacons." Retrieved October 10, 2013, from http://bgr.com/2013/10/03/apple-ibeacons-ios-7-advertising/

FTC. 2011. "Mobile Apps Developer Settles FTC Charges It Violated Children's Privacy Rule." from http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm

Gottipati, H. 2013. "With iBeacon, Apple is going to dump on NFC and embrace the internet of things." Retrieved October 10, 2013, from http://gigaom.com/2013/09/10/with-ibeacon-apple-is-going-to-dump-on-nfc-and-embrace-the-internet-of-things/

Hevner, A.R., March, S.T., Park, J., and Ram, S. 2004. "DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH," *MIS Quarterly* (28:1), pp 75-105.

Krasner, G.E., and Pope, S.T. 1988. "A description of the model-view-controller user interface paradigm in the smalltalk-80 system," *Journal of object oriented programming* (1:3), pp 26-49.

Kuechler, W., and Vaishnavi, V. 2012. "A Framework for Theory Development in Design Science Research: Multiple Perspectives," *Journal of the Association for Information Systems* (13:6), pp 395-423.

McCarthy, C. 2009 "ACLU chapter flags Facebook app privacy." *CNET*, from http://news.cnet.com/8301-13577_3-10318842-36.html

Reichhart, P., Pescher, C., and Spann, M. 2013. "A comparison of the effectiveness of e-mail coupons and mobile text message coupons for digital products," *Electronic Markets*), pp 1-9.

Sadeh, N., and Kelly, P.G. 2011. "User-controllable location privacy," *PriMo 2011 Workshop - 5th IFIP WG 11.11 International Conference on Trust Management,* N. Ahemd, D. Quercia and C.D. Jensen (eds.), Copenhagen, Denmark.

Shang, J., Yu, S., and Zhu, L. 2009. "Location-aware systems for short-range wireless networks," *Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on*: IEEE, pp. 1-5.

Sneps-Sneppe, M., and Namiot, D. 2013. "Smart Cities Software: Customized Messages for Mobile Subscribers," in: *Wireless Access Flexibility*. Springer, pp. 25-36.

Xu, H., and Bélanger, F. 2013. "Information Systems Journal Special Issue on: Reframing Privacy in a Networked World," *Information Systems Journal* (23:4), pp 371-375.

American Business Law Journal
Volume 45, Issue 3, 417–453, Fall 2008

POCKET Protection

Janine Hiller, France Belanger,** Michael Hsiao,*** and Jung-Min Park*****

I. INTRODUCTION

In December 2006 the online Web site Xanga.com was fined $1 million for failing to protect children's privacy as required under the Children's Online Privacy Protection Act (COPPA).[1] The Federal Trade Commission (FTC) estimated that 1.7 million accounts were created by underaged children without their parent's knowledge or consent.[2] Although the site asked for a person's age before completing registration, warning those under thirteen that they could not participate, nevertheless the system allowed those who subsequently entered birthdates indicating that they were under thirteen to simply continue the process of registration and to access and post information on the site.[3] Xanga also collected information from the children, including name, address, cell phone number, and instant messenger identification, which they posted in the child's online profile.

---

*Professor of Business Law, Virginia Tech, Blacksburg, Virginia. This research was supported, in part, by a grant from the National Science Foundation Cybertrust Program, #CNS-0524052. We would like to thank the participants in the 2007 Huber Hurst Research Seminar for their insightful comments and the University of Florida, Department of Management, for their sponsorship of the symposium.

**Professor, Accounting & Information Systems, Virginia Tech.

***Professor, Electrical & Computer Engineering, Virginia Tech.

****Assistant Professor, Electrical & Computer Engineering, Virginia Tech.

[1]Press Release, FTC, Xanga to Pay $1 Million to Violating Children's Online Privacy Protection Rule (Sept. 6, 2006), http://www.ftc.gov/opa/2006/09/xanga.shtm. COPPA is found at 15 U.S.C. §§ 6501–6506 (2000).

[2]*See* Press Release, *supra* note 1.

[3]*See id.*

The potential danger to young children was that this personally identifiable physical information was easily available online; the social networking site design encouraged communication and personal contact between registered users. Children could post profiles, pictures, and videos as well as communicate directly with other users.[4] The FTC fine against Xanga was the largest ever imposed under COPPA; the settlement of the complaint required Xanga to pay a $1 million fine, implement policies compliant with COPPA, file additional status reports, and submit to monitoring by the FTC.[5]

The Internet brings rich content to children and expands their horizons, but at the same time creates dangers and risks to their privacy and well-being. The recent massive and blatant failure of Xanga to follow COPPA is evidence that significant dangers to children still exist, despite the efforts of statutory protection. Protecting children's privacy today is essential because children are online at an increasingly younger age. A child's advanced technological sophistication that enables him to use the Internet does not match his worldly naïveté, and the dangers to children who share personal information are significant. Risks of harm can range from the threats of a child predator to the targeting and profiling of a commercial online marketer.

In Part II, this article describes the participation of children on the Internet, noting its exponential growth in recent years. Next, in Part III, the article examines the history of protecting children online. Part IV reviews the regulatory parameters of COPPA. COPPA was designed with the goal of interposing parental involvement in their child's electronic interactions by requiring parental consent for the collection of a child's personal information; ensuing regulations initially relied on the promise of emerging technologies to aid parents in this endeavor. The promise of a technological solution never materialized, however, and regulations setting standards for parental consent continue to be limited to the same methods as those available in 2000. Clearly, Internet and communications technology have progressed rapidly and significantly in over seven years, yet protection of children's privacy seems to have been left behind. Finally, in Part V, we propose a solution to this problem, providing evidence that the legal protections sought in COPPA can be implemented technically. This section

---

[4] *See id.*

[5] *Id.*

briefly describes POCKET (Parental Online Consent for Kids' Electronic Transactions), a technology concept we developed, under a National Science Foundation Cybertrust grant, to help protect children's privacy online.

A technological solution to protecting children online can be integrated into the legal framework, if parents, e-businesses, and regulators will take responsibility for its development, adoption, and use. We argue that it is possible, through the coordination of law and technology, to facilitate a parent's protection of his or her child in the online environment. The technology promise to protect children that seemed so near when COPPA was initially adopted should not be abandoned for less effective regulatory standards.

II. The Nature of Children Online

In 1997 14% of school-age children were online.[6] The FTC noted that the most prevalent activities for children online were "homework, informal learning, browsing, playing games, corresponding with electronic pen pals by e-mail, placing messages on electronic bulletin boards and participating in chat rooms."[7] Foreshadowing the future, the FTC commented in 1998 that the "most potentially serious safety concern is presented by the posting of personal identifying information by and about children . . . in interactive public areas . . . that are accessible to all online users."[8] A few short years later, 2003 statistics reported the number of children online by age: 19.9% between the ages of 3–4, 42.0% between the ages of 5–9, and 67.3% between the ages of 10–13.[9] The exponential increase in the numbers of children online, at increasingly younger ages, is an important reason to be concerned for their privacy.

Children participate in many activities online, accessing the Internet for information, help with homework, entertainment, and interaction.[10]

---

[6]FTC, Privacy Online: A Report to Congress 4 (1998) [hereinafter FTC 1998 Report].

[7]*Id.*

[8]*Id.* at 5.

[9]U.S. Dep't of Commerce, A Nation Online: Entering the Broadband Age, app. 2 (Sept. 2004), www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.pdf.

[10]Sonia Livingstone, *Children's Use of the Internet: Reflections on the Emerging Research Agenda*, 5 New Media & Soc'y 147, 149 (2003).

Even beneficial and benign uses by children can lead to or mask hidden dangers, however. For example, peer-to-peer (P2P) systems of communication, easily downloadable, can include bundled spyware that will collect information about children's online activities.[11] In addition, the expansion and popularity of social networking sites has created particular concern for parents.[12] Social networking sites are designed as online places where children can communicate with others with similar interests, a concept that can benefit children by increasing their knowledge, awareness, and personal communication skills, and simply being fun. Disney offers a new social networking site, for example, as it struggles to meet the popular demand for interactive features.[13] The site offers personalization for children, upgraded features for a fee, and retail sales. The inherent danger of social networking sites is that participation increases the chance that children will share personal information.

The gravest risk to children sharing information online is that it can allow predators to meet and harm them offline. It is estimated by the National Center for Missing and Exploited Children that one in seven children, ages ten to seventeen, are sexually solicited online.[14] Although parents may purchase and install filters to limit their children's online activities where a solicitation may be perceived as a greater threat, or where

---

[11]*See* Jessica Herdon, *Who's Watching the Kids—The Use of Peer-to-Peer Programs to Cyberstalk Children*, 1 Okla. J.L. Tech. 12, 13–15 (2004).

[12]In December 2005 the popular site MySpace recorded more Web page views than Google and eBay combined. Michael Nutley, *Corporates Target Youth Market via Emerging Media*, New Media Age, Feb. 6, 2006, at 14 (citing ratings from the Netview monthly Internet survey). *See also* Sue Shellenbarger, *How Young Is Too Young When a Child Wants to Join the MySpace Set?*, Wall St. J., Oct. 19, 2006, at D1 (discussing how to balance the benefits and dangers of new online social networking sites for young children). The American Medical Association has recently joined the discussion by adopting a policy that encourages physicians to engage and educate parents about the potential dangers to their children online. *AMA Adopts Plan to Help Protect Children From Online Harm*, U.S. Newswire, Nov. 14, 2006.

[13]http://disney.go.com/index (last visited June 1, 2008) (portal through which kids can enter contests, chat rooms, and more). A search for chatting reveals a statement that you can "Chat with your friends in Disney.com XD—the place to listen, watch, chat, and play all things Disney!" *See also* Merissa Marr, *Updated Disney.com Offers Networking for Kids*, Wall St. J., Jan. 2, 2007, at B1.

[14]*See* Jessica E. Vascellaro & Anjali Athavaley, *Foley Scandal Turns Parents Into Web Sleuths; Sales of Software that Tracks Kids Online Activities Soar; Cyber-Safety as a Job Benefit,* Wall St. J., Oct. 18, 2006, at D1.

sexually explicit material may be available,[15] it is the sharing of information without parental oversight, even on a children's site, that can pose the greatest risk.

Less sinister, yet undesirable, is the commercialization of a child's Internet use, where businesses collect personal information in order to create literal lifetime brand loyalty and target consumers. Children are not sophisticated enough to distinguish between advertising and unbiased content and can be convinced to share large amounts of personal information by the promise of a chance to win a small gift or the promotional antics of a cartoon character.[16] Also, marketing techniques can include creating profiles that can follow a child throughout his or her lifetime until adulthood and using those profiles to reach the parent through the child.[17] Hummerkids.com is a possible example of this trend. Although Hummers will obviously not be bought by children, www.hummer.com contains Hummer Kids, which includes coloring pages, a race where children choose their own Hummer, and a section where children can create their own Hummer. It is estimated that children under the age of fourteen influence 47% of family spending in the United States, representing $700 billion a year, perhaps explaining why more Internet sites that seem unrelated to children include children's pages.[18]

---

[15]*See id*.

[16]The results of an Annenberg Public Policy Center survey in 1999 are summarized in Press Release, The Annenberg Public Policy Center of the University of Pennsylvania, Free Gifts Could Entice Children Into Revealing Personal Family Information Online (May 16, 2000). For further examination of the results of this survey and the implications, see Joseph Turow, *Family Boundaries, Commercialism, and the Internet: A Framework for Research*, 22 Applied Dev. Psychol. 73, 79–80 (2001) (the effect of information release and its commercialization raises concerns). For a discussion of the cognitive age limitations of children, see Elizabeth S. Moore, *Children and the Changing World of Advertising*, 52 J. Bus. Ethics 161, 163 (2004). The impact of interactive advertising techniques, including online advertising, on young children is discussed in ChildrenNow, Interactive Advertising and Children: Issues and Implications (2005), http://www.childrennow.org/assets/pdf/issues_media_iadbrief_2005.pdf.

[17]*See* Livingstone, *supra* note 10, at 45–46. *See also* Joseph Turow, *Family Boundaries, Commercialism and the Internet: A Framework for Research*, 22 Appl. Dev. Psych. 73, 78–81 (2001) (information collection impacts the family as well as the child and results in dangers to the family unit and parental control).

[18]*Marketing to Children: Trillion Dollar Kids,* Economist, Dec. 2, 2006, at 66 ("Children are hedonists, inclined to make impulse buys and less likely to make educated purchasing decisions.").

The concern for protecting children online did not begin with the increasing commercialization of the Internet and the serious dangers of social networking. The potential harms to children sharing personal information online were recognized by the FTC early in the 1990s.

III. Privacy Problems in the Pre-COPPA World

In the 1990s the Internet and the World Wide Web had only begun ascending to national and international communication and commercial prominence. Yet, one of the initial concerns of users remains an issue today: the nature of privacy in the online environment, where collection of information about persons and habits is easy and far from transparent. Studies and surveys have consistently shown that the lack of privacy is a concern for consumers,[19] affecting how they use the Internet.

The early days of Web site development did not initially include protection for the less sophisticated child participant. In 1997 KidsCom operated a Web site that included "KidsCash" and "Find a Key Pal" activities, requiring children to register and provide their "name, birth date, e-mail and home addresses, and product and activity preferences"[20] in order to participate. Not only did the site collect this information from children, it also shared identifiers with other third parties. The Center for Media Education filed a complaint with the FTC, alleging deceptive actions by the KidsCom Web site in this method of information collection from children and its subsequent sharing practices with third parties.[21] Although the FTC decided not to pursue an action against the Web site because it had modified its information collection practices, the FTC did provide a staff opinion letter in which it established important standards for commercial entities who deal with children online.[22] It stated that it was a deceptive

---

[19]*See, e.g.*, Tom Buchanan et al., *Development of Measures of Online Privacy Concern and Protection for Use on the Internet*, 58 J. Am. Soc. Info. Sci. & Tech. 157, 158–59 (2007) (reviewing studies that document widespread concern for online privacy).

[20]Press Release, FTC, FTC Sets Forth Principles for Online Information Collection from Children (July 16, 1997), http://www.ftc.gov/opa/1997/07/kidscom.htm.

[21]*Id.*

[22]Letter from Jodie Bernstein, Director, Bureau of Consumer Protection, to Kathryn C. Montgomery, President, Center for Media Education, & Jeffrey A. Chester, Executive Director, Center for Media Education (July 15, 1997), http://www.ftc.gov/os/1997/07/cenmed.pdf.

practice to collect information from children for one reason yet use the information for another purpose and that it was "likely" to be an unfair practice to collect or release personally identifiable information from children without informed consent from a parent and the opportunity to restrict or prevent the collection and sharing of the child's information.[23]

A. The FTC's 1998 Privacy Study

The overall FTC approach to online privacy in the 1990s was to encourage Web sites to respect consumer privacy by voluntary self-regulation of information collection practices. In order to evaluate the effectiveness of the self regulatory approach, the FTC conducted a survey of Web site privacy practices in 1998, culminating in the report, "Privacy Online: A Report to Congress."[24] The FTC specifically addressed children's privacy concerns, and performed a separate study of children's Web sites in this survey.

The empirical results were striking: 89% of the Web sites studied collected personal information from children.[25] In order to entice children to share information, Web sites used offers of prizes, incentives of online chat rooms, and even the endorsement of imaginary characters in order to induce children to register and share personal information.[26] In fact, benefits were often available only upon registration.[27] Although the survey used a broad definition of a privacy policy, only 24% of the Web sites had such a policy, and only 8% of the sites stated that they informed parents of their information collection practices.[28] Forty-nine percent of the Web sites said they could share children's information with third parties.[29] A paltry three sites (of a sample of 212) required parental consent before information was collected from children.[30] The most common child protection

---

[23] *Id.*

[24] *See* FTC 1998 Report, *supra* note 6.

[25] *Id.* at 31.

[26] *Id.* at 33.

[27] *Id.*

[28] *Id.* at 34.

[29] *Id.* at 37.

[30] *Id.*

feature, followed by 23% of the sites, was simply to advise children that they should ask their parents before sharing information.[31]

To further evaluate the effectiveness of self-regulation, the FTC reviewed the two voluntary guidelines then available for businesses to use for standardized online child privacy practices. The Council of Better Business Bureaus' Children's Advertising Review Unit (CARU), and the Direct Marketing Association (DMA) each had established guidelines.[32] The CARU guidelines were acceptable to the FTC under the 1997 staff opinion letter, as they required notice and choice and providing parents with the opportunity to remove information about their children.[33] The CARU guidelines adopted a reasonableness standard to determine the acceptability of parental consent.[34] The FTC noted, however, that the CARU guidelines were not widely adopted by business.[35] The DMA guidelines were judged insufficient by the FTC as they were primarily aspirational in nature, without requiring fair information practices such as parental consent.[36]

The report gave guidance to Web sites for following effective privacy protection for children, listing notice/awareness, choice/consent, access/participation, and integrity/security.[37] Referencing the 1997 KidsCom staff opinion letter, the report emphasized that it is the *parent's* consent that is necessary, that adequate notice to the parent is a necessary precursor to collecting information from children, and that "actual or verifiable" parental consent is required when the information is to be shared with third parties.[38] Also relevant to future discussions of effectiveness, the report

---

[31]*Id*. at 34.

[32]*Id*. at 17.

[33]*Id*.

[34]*Id*.

[35]*Id*.

[36]*Id*. at 18.

[37]*Id*. at 12–14. These principles are broadly known for privacy protection, not just for children, and are widely recognized as Fair Information Practices. *See* Anita A. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751, 762 ("Fair information practices first promulgated in the 1970s are embodied in COPPA's requirements of notice, access, and security"); Jody Blanke, "*Safe Harbor" and the European Union's Directive on Data Protection*, 11 ALB. L.J. SCI. & TECH. 57, 70 (2000) (explaining that the FTC used the OECD Guidelines to identify five privacy principles, or "fair information practices").

[38]FTC 1998 REPORT, *supra* note 6, at 13.

noted that "online activities may be unique and unfamiliar to parents,"[39] and therefore notices to parents would need to be more robust. In this way, notices would "[empower] parents to monitor their children's interactions and . . . help protect their children from the risks of inappropriate online interactions."[40]

Not surprisingly, the FTC recommended that legislation be enacted requiring parental consent before commercial Web sites could collect information from children ages twelve and *under*.[41] The commission also recommended that parents of children *over* the age of twelve be notified of information collected and be given the opportunity to delete that information from a Web site database.[42] The FTC emphasized the role of parents and the necessity "of [legally] placing parents in control" of the information collected from their children.[43]

B. Early Child Privacy Cases Result in FTC Remediation

The FTC did not wait for the passage of legislation, but took the lead in addressing the conflict between privacy and the ease of electronic information collection from children in 1999. Under its Section 5 authority to prevent unfair and deceptive actions in commerce,[44] the FTC brought charges against two Web sites for collecting information in a deceptive manner.[45] In what the FTC calls the "First Internet Privacy Case,"[46] it filed a complaint against the Web site hosted by GeoCities. The GeoCities site contained individually created Web pages that were organized into "neighborhoods." Although the personal Web pages and areas of the site were free to users, GeoCities' business model was based on collecting information from consumers and selling that information to advertisers, who were

---

[39]*Id*.

[40]*Id*.

[41]*Id*. at 42.

[42]*Id*. at 42–43.

[43]*Id*. at 42.

[44]15 U.S.C. § 45(a)(1) (2000).

[45]*See* Allen, *supra* note 37, at 764–65.

[46]Press Release, FTC, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Information in Agency's First Internet Privacy Case (Aug.13, 1998), http://www.ftc.gov/opa/1998/08/geocitie.shtm.

then able to send targeted messages and ads to certain interest groups based on the identifying information.[47] The GeoCities site was hugely popular at the time of the complaint, with 1.8 million members and a listing in the top ten most visited Web sites.[48] Included in the numbers of members were approximately 200,000 children under the age of fifteen.[49] The site included the "Enchanted Forest" neighborhood and the "GeoKids Club" for children and required that children provide information including name, age, e-mail address, and gender, without any requirement of parental supervision or consent in order to participate.[50] These neighborhoods were maintained by third parties, although it would seem to users that they were GeoCities sites.[51] The GeoCities privacy policy stated that the information collected was never sold or shared, even though it regularly used the personal information for commercial gain. The FTC alleged that the privacy policy and practices were deceptive, and GeoCities subsequently entered into a consent decree to settle the charges.[52] The consent decree specifically addressed the online collection of information from children by requiring GeoCities to abstain from collecting personally identifying information from children ages twelve and under when it had "actual knowledge" that the child did not have parental consent to share the information.[53] It required a procedure to obtain express parental consent.[54]

The FTC brought a second complaint under its general authority in 1999 against Liberty Financial Companies for the practices on its younginvestor.com site.[55] The site required children to complete a survey in

---

[47]Complaint, FTC v. GeoCities, No. C-3850 (Feb. 5, 1999), http://www.ftc.gov/os/1999/02/9823015cmp.htm.

[48]*See id.*

[49]*Id.*

[50]*Id.*

[51]*See id.*

[52]Decision and Order, FTC v. GeoCities, No. C-3850 (Feb. 5, 1999), *available at* http://www.ftc.gov/os/1999/02/9823015.do.htm.

[53]*See id.*

[54]*See id.*

[55]Complaint, FTC v. Liberty Fin. Cos, No. C-3891 (Aug. 12, 1999), *available at* http://www.ftc.gov/os/1999/08/libertycmp.pdf.

order to receive a newsletter and to be eligible to win prizes. The survey asked for personally identifiable information such as name and addresses and also asked for financial information such as the child's weekly allowance and the types of investments that their family owned.[56] Although Liberty stated that the information would be anonymous, they held the identifiable information in a database. Adding further injury, the Web site never sent the newsletter or awarded the prizes.[57] The consent decree entered into by Liberty Financial defined "child" as someone under the age of thirteen, however, the order applied to those under the age of seventeen.[58] In addition, the order contained details regarding parental consent.[59]

These two consent decrees, entered into within months of each other, illustrated the challenge of designing an effective yet cost-efficient methodology for ensuring that parents are involved in protecting their children. The GeoCities decree defined acceptable methods of obtaining express parental consent as: (1) mail or fax, (2) an e-mail that included an electronically verifiable signature, (3) a secure credit card transaction, (4) any procedure authorized by law or regulation, or (5) "such other procedure that ensures verified parental consent and ensures the identity of the parent, such as the use of a reliable certifying authority."[60] It defined an electronically verifiable signature as "a digital signature or other electronic means that ensures a valid consent" by including authentication, integrity and nonrepudiation.[61] Furthermore, the decree allowed a Web site to adopt a screening procedure that sent an e-mail to the parent in order to obtain consent for the information collection.[62] The Liberty Financial decree adopted the same definition of an electronically verifiable signature, but substantially changed the definition of verifiable parental consent. In addition to the five methods described in the GeoCities settlement, the FTC included any "reasonable effort (taking into consideration available

---

[56]*See id*. at 1.

[57]*See id*. at 3.

[58]Decision and Order, FTC v. Liberty Fin. Cos., No. C-3891, at p. 3 (Aug. 12, 1999), *available at* http://www.ftc.gov/os/1999/08/libertydo.pdf.

[59]*Id*. at 4–5.

[60]*See GeoCities*, No. C-3850, *supra* note 52.

[61]*Id*.

[62]*Id*.

technology),'' as an accepted method of obtaining consent.[63] Clearly, the advent and application of new and effective methodologies was anticipated by the commission with their reference to available technology.[64]

IV. COPPA'S PRIVACY FRAMEWORK

Within months of the 1998 Report, Congress passed COPPA.[65] The swift enactment of the legislation was due in large part to the groundwork laid by the 1998 Report and the work of the FTC.[66] However, the legislation was proposed during a time of Internet regulation that included an Internet tax moratorium[67] and the limitation of children's access to pornography,[68] thereby overshadowing discussion of the comparably less controversial COPPA. The Congressional Record contains pages of debate about whether to limit children's access to harmful content and almost no legislative history to explain or supplement COPPA's statutory language. Comments summarily introduced by its cosponsor provide the most background.[69] The summary notes four goals:

> The goals of this legislation are: (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[70]

---

[63]*See* Liberty Fin., *supra* note 55.

[64]*Id.*

[65]Pub. L. No. 105-277, 112 Stat. 2681-2728 (1998) (codified as amended at 15 U.S.C. §§ 6501–6506 (2000)).

[66]*See* 144 Cong. Rec. E1861-01 (1998) (remarks of Rep. Edward J. Markey introducing the House version of the bill).

[67]Internet Tax Freedom Act, Pub. L. No. 105-277, 112 Stat. 2681-719 (1998) (codified as amended at 47 U.S.C. § 151 (2000)).

[68]Child Online Protection Act of 1998, 47 U.S.C. § 231 (1998).

[69]144 Cong. Rec. S12741-04 (1998) (remarks of Sen. Bryan, explaining that the bill went forward on voice vote from committee and no committee report was filed).

[70]*Id.*

Only the third goal, providing security for the information collected, a responsibility obviously associated with the collecting Web site, did not contain an element of parental involvement.

COPPA's focus on parental involvement is consistent with precedent; as a parent's participation in a child's education, health, and contracts is either legally sanctioned, permitted, or provided incentives in order to protect children in these important areas.[71] The following section focuses on the role of parental consent within the statutory framework of COPPA.

A. COPPA Definitions and Scope: Parental Consent Highlighted

Although the FTC suggested that the law apply in stages to children younger than seventeen, the law only protects a child under the age of thirteen.[72] Commercial online entities engaged in interstate commerce that collect information for themselves or on behalf of others are covered by COPPA.[73] The Web site operator must either direct its Web site or a part thereof toward children, or actually know that the information it collected was from a child,[74] in order for certain provisions to apply. The mere inclusion of a link to a different site that is targeted to children will not trigger the application of the statute.[75]

Personal information is defined as "individually identifiable information about an individual collected online"[76] and includes data that would allow the child to be individually contacted, either online or offline.[77] Thus, the online information that is personally identifiable specifically includes an e-mail address.[78] Name (first and last), address, telephone number, and Social Security number are also considered personally identifiable

---

[71]*See* Allen, *supra* note 37, at 772 (placing parents as gatekeepers is "arguably suitable" and is consistent with the Family Educational Privacy Act, for example); Danielle J. Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 151 (2001).

[72]Children's Online Privacy Protection Act, 15 U.S.C. § 6501(1) (2000).

[73]*Id.* § 6501(2) (definition of "operator").

[74]*Id.* § 6501(10)(A).

[75]*Id.* § 6501(10)(B).

[76]*Id.* § 6501(8).

[77]*Id.* § 6501(8)(F).

[78]*Id.* § 6501(8)(C).

information.[79] In addition, information aggregated about a child, *or their parents*, that is collected and matched with this identifying information, is also covered.[80]

Verifiable parental consent for the collection of a child's information may be obtained by "any reasonable effort (taking into consideration available technology)"[81] that results in parents receiving notice of the information collection, its use, and the site's privacy practices, together with the parent's consent to such use before information is collected from the child. The statute makes it clear that the parent may consent to future information collection as well as current collection.[82] In the summary of the law as it was presented for adoption, it was noted that parental consent

> should be interpreted flexibly, encompassing "reasonable effort" and "taking into consideration available technology." Obtaining written parental consent is only one type of reasonable effort authorized by this legislation. "Available technology" can encompass other online and electronic methods of obtaining parental consent. Reasonable efforts other than obtaining written parental consent can satisfy the standard. For example, digital signatures hold significant promise for securing consent in the future, as does the World Wide Web Consortium's Platform for Privacy Preferences.[83]

Disclosure of information occurs in one of two ways, either by the release of information in identifiable form, which would include sharing of information for marketing purposes, for example, and by making the personally identifiable information available publicly.[84] The statute lists the actions of publicly posting the information on the Internet, on a home page, or through pen pals, e-mail, message boards, or chat rooms, as disclosure.[85] Comments in the House of Representatives noted that "the public posting of children's identifying information in chat rooms and other online forums may pose safety concerns, and the bill simply protects against those things happening."[86]

---

[79]*Id.* § 6501(8)(A), (B), (D), & (E) (respectively).

[80]*Id.* § 6501(8)(G).

[81]*Id.* § 6501(9).

[82]*See id.* ("and the subsequent use of that information").

[83]144 Cong. Rec. S12741-04 (1998).

[84]COPPA, 15 U.S.C. § 6501(4) (2000).

[85]*Id.* § 6501(4)(b).

[86]144 Cong. Rec. H9902-01 (1998).

As we know years later, protecting children in online forums is a worthwhile and necessary goal, yet a simple implementation has not been found.

B. Unfair and Deceptive Practices Defined in COPPA

COPPA makes it unlawful for businesses (an unfair and deceptive practice) to collect information from children in a way that conflicts with the statute and any regulations adopted by the FTC in its furtherance.[87] COPPA requires businesses to:

1. Provide notice of information collection practices, including use and disclosure practices,[88]
2. Obtain prior verifiable parental consent for the collection, use, or disclosure of the information,[89]
3. Facilitate parental access to information collected, the right to delete the information, and the ability to prohibit further collection,[90]
4. Refrain from conditioning a child's participation in online activities on disclosing information unless it is reasonably necessary,[91] and
5. Protect and maintain the accuracy and security of the information collected.[92]

Exceptions to the requirements are based on the limited use of that information and include a one-time response to a child when that information is not retained by the business and the child is not recontacted by the business.[93] In addition, the information may be collected without parental consent when it is used to contact the parent to obtain consent, for the safety of the child, for the secure operation of the site, or other legally authorized reasons.[94]

---

[87]COPPA, 15 U.S.C. § 6502(c) (2000).

[88]*Id.* § 6502(b)(1)(A)(i).

[89]*Id* § 6502(b)(1)(A)(ii).

[90]*Id.* § 6502(b)(1)(B).

[91]*Id.* § 6502(b)(1)(C).

[92]*Id.* § 6502(b)(1)(D).

[93]*Id.* § 6502(b)(2).

[94]*Id.* § 6502(b)(2)(D).

COPPA includes a provision for the establishment of safe harbors "issued by representatives of the marketing or online industries,"[95] when approved by the FTC, as "incentives for self regulation."[96] Participation in and meeting the expectations of an approved safe harbor program is deemed to be compliance with the statute. At the present time there are four safe harbor programs approved by the FTC.[97]

The FTC[98] and state Attorneys General have enforcement power,[99] and the FTC was directed to adopt regulations regarding these practices.[100] Regulations to implement COPPA, and the approval of safe harbors, are discussed in the following sections.

C. The Protracted Development of COPPA Regulations

The FTC proposed rules to enforce COPPA in 1999.[101] Because of particular interest in the application of "verifiable parental consent," the FTC held an additional workshop focused on this provision.[102] The final rules, and the temporary rule for obtaining verifiable consent, were made effective as of April 2000.[103] This article focuses on those aspects of the regulations affecting the nature of parental consent and the potential for using technology for obtaining that consent. In that regard, the history of the development of the standards, the comments of industry, and the expectations expressed as the rule developed, are relevant.

---

[95]*Id.* §6503(1) (or other entities).

[96]*Id.* § 6503(b)(1).

[97]*Id.* § 6503(b)(2). The four approved safe harbor programs are: The Children's Advertising Review Unit, Entertainment Software Rating Board, TRUSTe, and PRIVO. *See* FTC Safe Harbor Program, http://ftc.gov/privacy/privacyinitiatives/childrens_shp.html (last visited Mar. 21, 2008).

[98]COPPA, 15 U.S.C. § 6505(a) (2000) (various other financial agencies have authority to enforce the provisions under subsequent subsections of § 6505).

[99]*Id.* § 6504.

[100]*Id.* § 6506.

[101]Children's Online Privacy Protection Rule, 64 Fed. Reg. 22750 (proposed Apr. 27, 1999) (to be codified at 16 C.F.R. § 312).

[102]Press Release, FTC, FTC to Hold Public Workshop on Appropriate Methods to Obtain Parental Consent in Conjunction with Rulemaking on Children's Online Privacy Protection Act (June 23, 1999), http://www.ftc.gov/opa/1999/06/kidswork.htm.

[103]Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2008).

Parental consent must be informed; the standard proposed by the FTC was that notice must be reasonably designed based on available technology.[104] Possible methods for providing notice included "sending the notice by postal mail, sending the notice to the parent's e-mail address, or having the child print out a form to give to the parent."[105]

The proposed regulation pertaining to the method of parental consent, itself, was linked to the available technology, following the language in COPPA. In developing the regulations more fully, the FTC took the position that it could not at that time adopt a particular technology and requested input regarding the "feasibility, costs and benefits" of different technical methods.[106] Possible methods noted by the commission included a physically produced and mailed consent form signed and returned by the parent (mail or fax), the use of a credit card transaction, a toll free number for parents to call, and a digitally signed e-mail.[107] At that point, the commission also asked for comments about the use of e-mail for other limited types of consent.[108]

A substantial number of comments focused on the potential for technology to assist businesses in obtaining parental consent; however, no clear consensus emerged from this input.[109] One group of commentators agreed that the old-fashioned physical consent form was the most dependable and verifiable; the American Psychological Association (APA) advocated the use of this method based on a "particular concern" that "[c]hildren under the age of 13 do not have the developmental capacity to understand the nature of the request for information that is being made by a Web site and may, unknowingly, pass along information not intended for distribution or collection by their parents."[110] Although this method would slow the process of obtaining consent, it would provide an oppor-

---

[104]Children's Online Privacy Protection Rule, 64 Fed. Reg. at 22753 (explaining proposed rule § 312.4(2)(c)).

[105]*Id*.

[106]*Id*. at 22756.

[107]*Id*.

[108]*Id*.

[109]*See id*. at 59888 & 59899 (Nov. 3, 1999) (to be codified at 16 C.F.R. § 312) (final rule).

[110]Letter from Jeff McIntyre, Legislative & Fed. Affairs Officer, Am. Psychological Ass'n., to Donald S. Clark, Sec'y, FTC (June 11, 1999), http://www.ftc.gov/privacy/comments/apa.htm.

tunity for parents to increase their involvement, providing an opportunity to educate children about the online environment. Interestingly, the APA's comments recognized the potential burden of requiring a signed, physical, writing for consent, but argued that this would provide an incentive for business to develop "secure, affordable technology using digital signatures."[111]

The use of e-mail to obtain parental consent was seen by commentators as problematic. This method was identified as the easiest and least costly for businesses, but was also recognized as having the greatest potential for abuse.[112] Several commentators provided information that parents and children at that time used the same e-mail address and that easily obtainable e-mail addresses would lead to falsification of consent by the child.[113] The use of a credit card transaction to identify the person as a parent was viewed in a similar light; comments noted that not all parents used credit cards, and one credit card company emphasized that credit cards should not be used for identification.[114]

1. 2000 Temporary Final Rule

Adopting the final rule, the FTC stated the goals of "maintaining children's access to the Internet, preserving the interactivity of the medium, and minimizing the potential burdens of compliance on companies, parents, and children."[115] It sought to balance these goals with the protection of children online[116] by making its final rule temporary, based on a "sliding scale" method of consent "until secure electronic methods [became] more available and affordable."[117]

The final temporary rule adopted a standard for consent as follows:

> An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any consent must be rea-

---

[111] *Id.*

[112] Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59900.

[113] *Id.*

[114] *See id.* at 59900–01.

[115] *Id.* at 59889.

[116] *See id.*

[117] *Id.* at 59901.

> sonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.[118]

The rule then specified the following methods to meet this standard: a signed consent form that is mailed or faxed, use of a credit card in a transaction, a toll-free number to be called by a parent that is staffed with trained personnel, digital signature using public key cryptography, or an e-mail utilizing a password or personal identification number (PIN).[119] Importantly, the final rule also included a provision that allowed businesses to adopt a less rigorous standard until April 21, 2001. The less stringent standard allowed the use of an e-mail consent method if (1) the information collected is not shared with third parties, (2) the e-mail is accompanied by additional steps to determine the parent's identity (specifically mentioned were an e-mail, mail, or telephone confirmation), and (3) the parent is given notification that they may revoke previous consent.[120] This method has come to be known as the "e-mail plus" method of obtaining parental consent.[121] While the methodology became known as a "sliding scale," the rule actually encompasses a two-tier standard, based primarily on whether the information is shared externally. Noting the number of technologies already identified in the comments, the FTC believed that the sliding scale was only necessary in the short term, as "with advances in technology, companies will soon be able to use more reliable verifiable electronic methods in all of their transactions."[122] In the meantime, the sliding scale "[provided] operators with cost-effective options until more reliable electronic methods [became] available and affordable, while providing parents with the means to protect their children."[123]

---

[118]16 C.F.R. § 312.5(b) (2008).

[119]*Id.* § 312.5(b)(2).

[120]*Id.*

[121]*See* Garber, *supra* note 71, at 184 n.255.

[122]Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59902 ("Comments and testimony at the workshop showed that digital signatures and other reliable electronic methods are likely to be widely available and affordable within approximately a year . . . ample time for these mechanisms to develop and become widely available").

[123]*Id.*

2. 2001 Review

In 2001 the FTC undertook an empirical study of the privacy policies of Web sites targeted to children[124] and also requested comments to review the temporary sliding scale for obtaining parental consent, soon slated to expire. Although the study of Web sites focused on the privacy policies of the sites, it also collected information about the use of parental consent mechanisms referenced in the privacy policy. Of those sites that disclosed their practices in the policy, the study found that half of the Web sites utilized the print and confirm procedure, and half used e-mails to parents. Seventeen percent used telephone verification, and 31% used some other method.[125] The number of Web sites collecting personal information from children dropped from 89% in 1998, to 72% in 2001.[126]

In response to its request for comments, the FTC received twenty-one submissions concerning whether the sliding scale should be extended or made permanent.[127] Although the comments varied considerably, most commentators stated the opinion that the sliding scale should be extended because the predicted advance in available technology had not occurred.[128] In contrast to the FTC's optimistic assumptions two years earlier, comments described the technology as "nascent,"[129] warning that "no widely and economically feasible verification technology even appears to be on the near horizon."[130]

Slow acceptance and adoption of technology by consumers and parents was cited as one reason for the lack of progress toward a technical solution to protecting children online.[131] The Entertainment Software

---

[124]*See* FTC, Protecting Children's Privacy Under COPPA: A Survey on Compliance (2002), *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf [hereinafter FTC 2002 Report].

[125]*Id.* at 12.

[126]*Id.* at 3.

[127]*See* Children's Online Privacy Protection Rule: Public Comments Received, http://www.ftc.gov/privacy/coppa2/comments/index.html (last visited Mar. 21, 2008).

[128]Children's Online Privacy Protection Rule, 67 Fed. Reg. 18818, 18820 (Apr. 17, 2002).

[129]Letter from Jill Luckett, Vice President, Nat'l Cable & Telecomm, Ass'n., to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/ncta.htm.

[130]Letter from Magazine Publishers of America to FTC, http://www.ftc.gov/privacy/coppa2/comments/mpa.htm (last visited Mar. 27, 2008).

[131]*See* Luckett, *supra* note 129.

Ratings Board, certified as a safe harbor, noted that they were open to adopting more technically sophisticated measures such as digital signatures, but that "such mechanisms have been of limited utility since few parents are familiar with the technology, and those few have found the technology difficult to use. Thus, from a parent's perspective, the use of digital technology tools has been unattractive and impractical."[132]

Several commentators advised against extending the sliding scale, however, and one well-known trust organization warned that "[c]hoosing to extend the compliance date every two years because new technological solutions have not been widely adopted, is likely to create a regulatory environment that does not place pressure or give incentive to companies to invest and use such systems."[133] Other comments emphasized that the online environment was no less dangerous for children than in the previous two years, and the need to protect children was even more pressing, especially with regard to the availability of public information in places such as chat rooms.[134]

In support of maintaining the flexibility of the sliding scale, especially the e-mail-plus method, principals of Cyberangels, an online safety organization, said:

> Parents have been slow to respond to requests for consent. From busy soccer moms and dads to corporate workers and executives, parents have overwhelming demands on their time. The easier the consent process is, the better the response rates will be—always keeping in mind the need to have the consent "verified."[135]

The FTC temporarily extended the sliding scale for another three years, until April 2005, noting that "[s]ecure electronic mechanisms and/or infomediary services for obtaining verifiable parental consent are not yet widely available at a reasonable cost."[136]

---

[132]Letter from Marc E. Szafran, Vice President, Entertainment Software Rating Board, to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/esrb.htm.

[133]Letter from Rebecca J. Richards, Director, TRUSTe, to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/truste.htm.

[134]*See* Letter from Jorian Clarke, President, Circle 1, to FTC (Nov. 30, 2001), http://www.ftc.gov/privacy/coppa2/comments/caru.htm (citing increasing number of children online, increasing pornography, and decreasing choices).

[135]Letter from Parry Aftab, Esq. & Nancy L. Savitt, Esq., to FTC, http://www.ftc.gov/privacy/coppa2/comments/aftab.htm (last visited Mar. 27, 2008).

[136]Children's Online Privacy Protection Rule, 67 Fed. Reg. 18818, 18819 (Apr. 17, 2002).

3. 2005 Review

In 2005 the FTC undertook a second review of COPPA rules and proposed making the sliding scale rule permanent.[137] Comments were solicited about the availability of technical methods for obtaining parental consent in both a general review and specific sliding scale requests for comments. Specific technologies mentioned included digital signatures, digital certificates, digital credentialing, P3P, and infomediaries.[138] Twenty-five comments were submitted about COPPA in general, and ninety-one comments were submitted specifically concerning the sliding scale.[139]

The FTC distinguished between form-based and non-form comments in assessing the input. Forty-eight comments opposing consent by e-mail were discounted, as the FTC explained that the rule did not allow bare e-mail consent, but required the e-mail-plus method.[140] The majority of non-form comments favored retaining the sliding scale rule, with or without some modification.[141]

The FTC once again noted the general concurrence that electronic verification technology was neither widespread nor cost effective and that the future of these technologies was unpredictable.[142] The technologies mentioned included digital signatures, public key infrastructure, P3P, and infomediaries.[143] Digital signature technology uses a mathematical formula to encrypt a message from a person that can only be decrypted with a unique formula. Thus, one may be sure that the person who sends the message, or in the case of COPPA the person who grants parental consent,

---

[137]*See* Children's Online Privacy Protection Rule, 71 Fed. Reg. 13247 (Mar. 15, 2006).

[138]*See id* at 13255.

[139]*Id*. at 13247.

[140]*Id*. at 13248–49.

[141]*See id*.

[142]*Id*. at 13255.

[143]A more detailed description of these technologies is beyond the scope of this article. For more detailed information on privacy-enhancing technologies such as those mentioned, particularly P3P, see generally Noushin Ashrafi & Jean-Pierre Kuilboer, *Privacy Protection Via Technology: Platform for Privacy Preferences (P3P)*, 1 Int'l J. E-Bus. Res. 56 (2005); Kimberly Rose Goldberg, *Platform for Privacy Preferences (P3P): Finding Consumer Assent to Electronic Privacy Policies*, 14 Fordham Intell. Prop. Media & Ent. L.J. 262 (2003).

is identified and the message is authentic. Public key infrastructure supports encryption; it is a method by which the mathematical scrambling known as encryption may be matched with the person sending the message. P3P, or Platform for Privacy, is a system of privacy setting standards that operationalizes privacy policies of participating Web sites into a format that can be read by a computer automatically and compared with preferences set by a user; if the policy does not meet the privacy preferences set by the user, then a notification message is displayed. An infomediary, as used in this context, is an entity that serves the function of certifying trustworthiness between two parties by acting as a middleman for the negotiation of whether or not to share information.[144] The conclusion reached after reviewing these choices was that no single technology was universally cost effective, available, and effective for obtaining parental consent.[145]

One group of comments predicted that a permanent rule would actually promote the development of more secure methods of parental consent, as the temporary nature of the rule discouraged investment because of regulatory uncertainty.[146] Commentators generally agreed that the internal use of personal information by Web sites posed the least danger for children and that less costly parental consent mechanisms for this type of information collection and use served to preserve content for children on the Internet.[147] Furthermore, it was stated that the sliding scale responded to the increased risk of public disclosure or sharing of children's information by imposing more secure parental consent mechanisms for these uses.[148]

Thus, in March 2006 the FTC retained the sliding scale for obtaining parental consent, stating that, "[in]n light of the unpredictability of tech-

---

[144]An "infomediary" is not defined by the FTC and is sometimes called an information intermediary in other disciplines. *See* Robert Garfinkel et al., *Secure Electronic Markets for Private Information*, 36 IEEE Transactions Sys., Man & Cybernetics 461, 462 (2006) (trusted information intermediary).

[145]P3P lacked an identity function and was not designed to obtain parental consent for children's information; digital signatures and infomediaries were not widely available or cost effective.

[146]*See* Children's Online Privacy Protection Rule, 71 Fed. Reg. at 13256–57.

[147]*See id.*

[148]*Id.* at 13257.

nological advancement and the benefits of decreasing regulatory uncertainty, the Commission has determined to retain the sliding scale indefinitely while it continues to evaluate developments."[149] In conclusion, the FTC noted that it maintained the right to modify the rule in response to future developments.[150]

4. 2007 Report

In February 2007 the FTC reported to Congress as required by COPPA and concluded that the administrative rules provided a "workable system" for providing online privacy and safety to children.[151] The report relied on the 2006 comments and review, described earlier, but noted additional future challenges.

First, the emergence and popularity of social networking sites was noted as a particularly risky development, enabling child predators to identify and contact children.[152] The Xanga case prosecution was discussed in this light, and the FTC expressed the opinion that the significant penalty imposed would act to guide other social networking sites to protect children and deter them from making similar mistakes. As Xanga involved children falsifying their ages to register and gain access to the Web site, it is interesting that other sections of the report commented about the ease of age falsification when low-technology methods are used. In contrast, the Commission noted that "[c]ontinued concerns about children's online safety may prompt the more rapid development of age verification technology. The Commission will monitor closely any such developments, and will update its business guidance accordingly if and when such technology becomes more widespread."[153]

The report also identified the convergence of technologies as a future area of concern. Growing access to the Internet by mobile devices will increase the difficulty for parents to supervise their children's activities on-

---

[149]*See id.*

[150]*See id.*

[151]FTC, Implementing the Children's Online Privacy Protection Act 28 (2007), *available at* http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

[152]*Id.* at 25–27.

[153]*Id.* at 13.

line.[154] The FTC promised to monitor these developments. Lastly, the FTC concluded that the "failure to develop more secure electronic mechanisms or infomediaries to verify parental consent poses an additional technological challenge."[155]

V. Improving the Effectiveness of Parental Consent in COPPA

Parental consent is the lynchpin of COPPA; rather than adopt a draconian law that prohibited information collection from children, Congress relied upon a flexible approach to obtaining parental consent. Yet, the parental consent formulation of the law has been criticized for being unrealistic, costly,[156] and more beneficial to businesses than to parents.[157] Although several studies subsequently reviewed Web site privacy policy compliance with COPPA requirements,[158] the important issue of parental consent methodologies and effectiveness has not been similarly studied or analyzed. Instead, the FTC anticipated the evolution of a technological solution to more powerfully and effectively support this element of the law, a means that never developed. The following sections review concerns and challenges and describe a possible solution.

A. Initial Concerns Regarding Complexity and Evasion

Debate about the efficacy of COPPA arose soon after its adoption.[159] Criticisms included the cost to businesses, the lack of parental ability to mon-

---

[154]*Id.* at 27.

[155]*Id.* at 29.

[156]Joshua Warmund, *Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act*, 11 Fordham Intell. Prop. Media & Ent. L.J. 189, 208–11 (2000).

[157]Joseph A. Zavaletta, *COPPA Kids, Cookies & Chat Rooms: We're From the Government and We're Here to Protect Your Children*, 17 Santa Clara Computer & High Tech. L.J. 249, 270–72 (2001).

[158]*See generally* FTC 1998 Report, *supra* note 6; FTC 2002 Report, *supra* note 124. *See also* Tess Koleczek, *Children's Section On Children's Privacy on the Internet*, 6 U.C. Davis J. Juv. L. & Pol'y 79, 85–90 (2001) (containing a short study, including measures, for obtaining parental consent).

[159]*See, e.g.*, Mark. D. Robins, *Coping with COPPA: Privacy, Children, and the Internet*, 17 Computer Law. 17, 17 (2000) (noting that the regulations "represent a highly complex labyrinth of tests, required procedures, exceptions, safe harbors, and traps for the unwary").

itor, and the ease with which children could manipulate consent mechanisms.[160] Dire consequences were predicted; Web sites would simply close their online doors to children under age thirteen because it would be too difficult to comply with the burdensome regulations and too expensive to obtain parental consent.[161] Amid the initial confusion, Disney announced that it would bar children under age thirteen from its chat rooms.[162] From the consumer side, there was concern that the law primarily protected businesses while giving parents, on behalf of their children, neither the tools of control nor the power of enforcement.[163] At this early date, at least one commentator concluded that the parental consent measures were impractical, inadequate, and constitutionally suspect.[164] In contrast, the emphasis on parental involvement led others to believe that the law could be an effective legislative tool to protect children.[165] A period of time after COPPA's effective date however, commentators continued to question whether the consent methods were effective, restating concerns that children would be able to easily enter false ages to avoid restrictive Web sites and that parental involvement was problematic because continuous monitoring was too onerous and burdensome.[166]

B. Current Environment in Light of COPPA

Clearly, Web sites have generally become more careful about collecting information from children after the passage of COPPA. However, the failure to develop a robust technical means to protect children has thwarted

---

[160]*See* Andrea M. Matwyshyn, *Technology, Commerce, Development, Identity*, 8 MINN. J.L. SCI. & TECH. 515, 547 (2007) (discussing the difficulty of parental monitoring); Warmund, *supra* note 156, at 207–10 (detailing the cost and ease of child manipulation).

[161]*See* Melanie L. Hersh, *Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L.J. 1831, 1855–68 (2001).

[162]*Id.* at 1866.

[163]*See* Zavaletta, *supra* note 157, at 270–72.

[164]*See* Warmund, *supra* note 156, at 213–16.

[165]*See* Garber, *supra* note 71, at 186–87 ("COPPA serves to increase children's safety online and to protect their privacy in the most effective way that the Internet currently affords").

[166]*See* Allen, *supra* note 37, at 768–69; Rachael Malkin, *How the Children's Online Privacy Protection Act Affects Online Businesses and Consumers of Today and Tomorrow*, 14 LOY. CONSUMER L. REV. 153, 167–68 (2002).

the goal of COPPA regulations regarding parental consent. Children are accessing the Internet more frequently and are visiting a wider variety of Web sites, not all of which are directed at children. Therefore, those Web sites may not employ strong methods of age verification. Businesses are building on the fact that children can affect the purchasing decisions of their family, and are increasingly offering child-oriented activities to general-audience Web sites. In addition, Web sites seem to have overcome their initial misgivings about compliance and the regulatory burden, perhaps in light of the potential commercial value of young consumers. Disney, having initially decided to limit the offerings of its Web sites to children under age thirteen, recently announced the launch of a new site that incorporates new interactivity and increased opportunities for personalization.[167]

In light of the trend for Web sites to become increasingly interactive in order to attract young consumers, one might expect that parallel technologies to protect children and enable parents to control their online activities would also emerge. Such has not been the case. Today, Web sites may have learned from the Xanga case that they should not allow a visitor to go back and reenter a different age, thereby bypassing the verification process, but they have taken few steps beyond the simple use of cookies to prevent this practice. The technical sophistication of children continues to trump these basic techniques,[168] as the basic knowledge of how to clear the cache will allow a child under age thirteen to circumvent the age falsification preventive method of using cookies.

While children become more adept technically, parents seem to fall behind.[169] They are uncomfortable with even basic technical measures, such as using the history browser button to see which sites their child has visited. Parents most often use nontechnical means to monitor their child's Internet usage, such as placing the computer in a common room in the house. Parents are almost completely unaware of the four self-regulatory (safe harbor) programs approved by the FTC. There is little indication that

---

[167]Marr, *supra* note13, at B1.

[168]Although this evidence is purely anecdotal, we have been informed on numerous occasions by students that any ten-year-old boy knows how to clear the browser history button and the cookie file.

[169]Our focus group studies indicated that parents have not heard of the safe harbor groups. *See* Robert Crossler et al., *Parents and the Internet: Privacy Awareness, Practices, and Control*, 2007 Proc. Am.'s Conf. Info. Sys. 3 (on file with authors).

the self-regulatory programs can create any trust by parents who are unaware of their existence.[170] The goal of parental involvement is therefore unassisted by technology or self-regulatory groups. Lastly, parents have no mechanism to individually enforce any deficiencies by Web sites that they might discover. Although the FTC has sought enforcement against high-profile and serious violators, it has limited resources, and has brought only eleven cases in seven years.[171]

If COPPA is to protect children online by means of parental involvement, then new tools are needed to assist them, technical methods that will empower parents to assert control over Web site practices, and even their own, technically sophisticated children. The regulations anticipated this technical development, and it is essential that these tools develop if COPPA is to become truly effective in protecting children in today's online environment.

C. Conceptualizing Parental Verification and Consent

Conceptualizing the implementation of parental consent is an important step toward determining how to increase the effectiveness of COPPA regulations in order to meet the goal of protecting children online. The operation of Web sites today, under COPPA, can be expressed by the illustration in Figure 1, showing that the Web site and the child are the primary parties in direct communication.

As the illustration shows, the Web site is responsible for obtaining consent from the parent. The means of obtaining parental consent puts the Web site in the middle of the process, between the parent and the child, quite different from the original intent under COPPA that anticipated that the involvement of the parent with the child would act as an educational and monitoring function. Figure 1 also shows that the Web site is in charge of the communications. The parent could communicate with the Web site and grant or deny consent and the child may never be directly involved with the parent. Of course, the parent will know of the child's interest and will have the opportunity to discuss the decision and the online activities

---

[170] *Id.*

[171] The FTC Web site has a list of these cases. FTC Privacy Initiatives, http://ftc.gov/privacy/privacyinitiatives/childrens_enf.html (last visited Mar. 21, 2008).

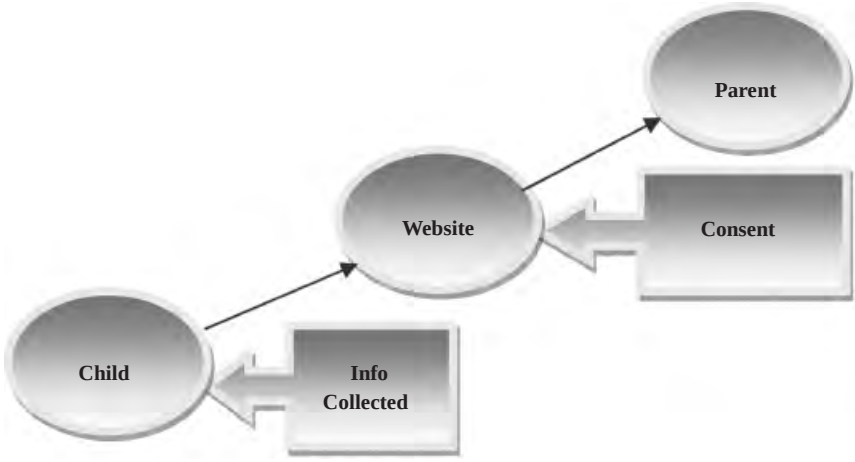


Figure 1. Present Consent Mechanism

with the child later. And, as the Xanga case shows, if COPPA compliance fails, the parent will be unaware of the violation and unable to provide a buffer between the Web site and the child to prevent the information collection.

However, consider the rearrangement of the process shown in Figure 2, which would change the dynamics of the interaction between child, parent, and Web site.

Obviously, if the parent could be involved with the transaction between the child and the Web site, providing a mature and protective influence, then it would satisfy the intent of COPPA and provide protection for the child. The reality is however, that parents cannot always be present, mediating every Web interaction, when their child is online.

If technology could provide a means for mediation, it could act as an automatic predetermined proxy for the mature decision making of the parent regarding information collection.

The conceptual illustration shown in Figure 3 proposes that it would be possible for technology to allow a parent to control the child's ability to share information by software installed on the computer, blocking access to the Web site unless the Web site meets the requirements preset by the parent. If the child wishes to access the site, then he/she will need to ask the parent to unblock the site, thereby instigating the communication between

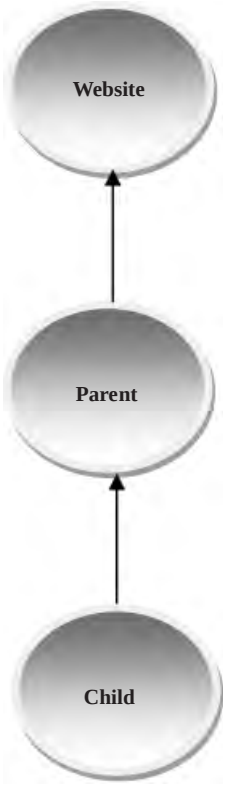


Figure 2. Parental-Mediated Consent

parent and child about online activities. The heavier arrow between the Web site and the computer indicates that the information collected by the Web site is only that allowed by the parent, and the Web site collects no information directly from the child.[172]

---

[172]The technology of P3P is a related example of this concept; however, it does not include exchange of specific, user-generated information between the user and the Web site in the transaction. The weakness of P3P is that it does not account for the necessary authentication and security when information may be exchanged on an open network. For a basic description of P3P, see Mary Anne Patton & Audun Josan, *Technologies for Trust in Electronic Commerce*, 4 Elec. Com. Res. 9, 12–13 (2004).

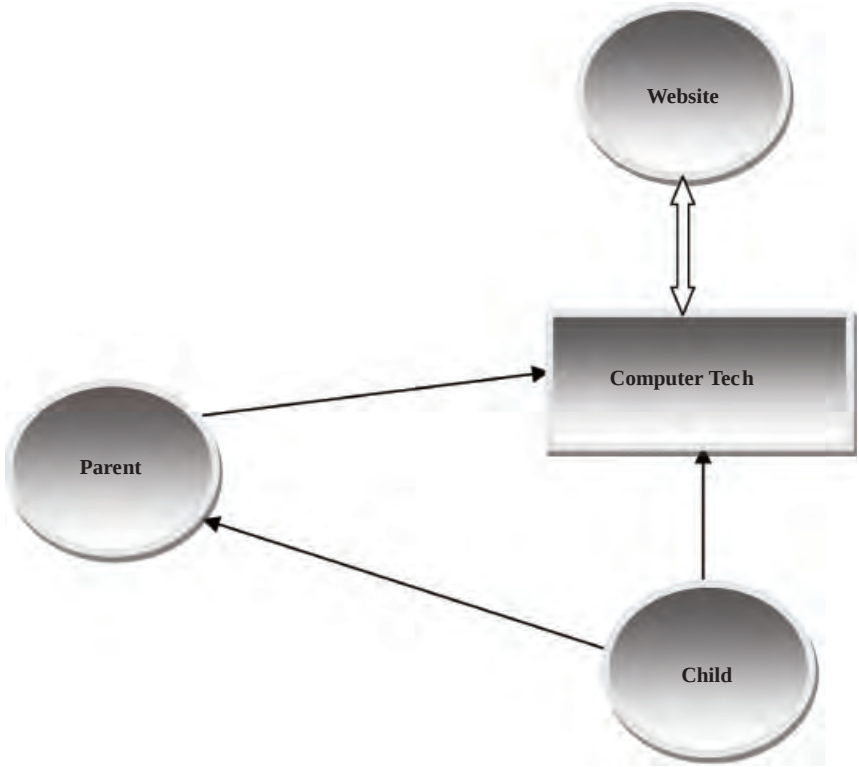


Figure 3. Technology-Aided Consent

D. A New Technical Concept: POCKET

POCKET is a proof-of-concept[173] system we developed that would allow for the implementation of the concept described above in a more sophisticated and robust manner. POCKET is a technical solution to obtaining parental consent. In the following section, the system is described briefly, in a nontechnical manner, to show how it would meet the conceptual needs of COPPA, obtain parental consent, and protect children. The benefit of the POCKET system is that it puts control back in the hands of the parent, making the parent the focal point of child protection, as originally envisioned in COPPA.

---

[173]A proof of concept is not a fully developed product; it functions in the lab environment to show that it is technically possible to achieve the result.

POCKET is composed of two parts, the parent/child side and the Web site side, and consists of two stages, the registration stage and transaction stage. In the registration stage the parent must first obtain and install the software on the home computer that is used by the child. The software will work through the browser on the home computer to implement the system. When the parent obtains the software he or she must provide identification and register, creating a password that will be used in any future interactions. The merchant installs similar POCKET software, thereby allowing automatic communication between the two parties (by computer interactions). During the registration process, the parent enters specific choices about what information about the child may be collected and whether the information may be shared. The Web site also specifies its information collection and sharing practices during its registration process.

In the transaction phase, when a child visits a Web site, the parent/child POCKET software interacts automatically and transparently with the merchant POCKET software, identifying that there is a user under the age of thirteen[174] and implementing preset instructions about what personally identifiable information, if any, can be given to the Web site and whether the information can be shared. If the Web site requests information through POCKET that does not match the choices made by the parent on behalf of the child, then POCKET automatically blocks the Web site. If the Web site collection and parent preferences match, then POCKET automatically transfers the child's information from the child's computer to the Web site. A log is kept on the parent/child's computer so that the parent can check at any point in time to determine where the child has visited and what information has been shared. The system is illustrated conceptually in Figure 4.

---

[174]In addition, POCKET also addresses the issue of security and trustworthiness between the parent/child and Web site computers. POCKET incorporates transparent authentication protocols so that the Web site can be assured that the information that is transferred from the child's computer is authentic and secure. As the parent/child's computer transfers information to the Web site, the POCKET system acts as the trusted third party, the certificate authority, to incorporate a digital signature based on public key encryption to identify the sender. This is important because the Internet, being a public and open architecture, is not a secure environment. Others may intercept and change the communication, potentially attacking the Web site and endangering the child's information, unless security measures are taken. The use of a "ticket," the combination of the digital signature attached to the message, is a process that ensures the integrity of the message and provides for nonrepudiation. Importantly, the use of the ticket is automated and requires no additional action by the parent.

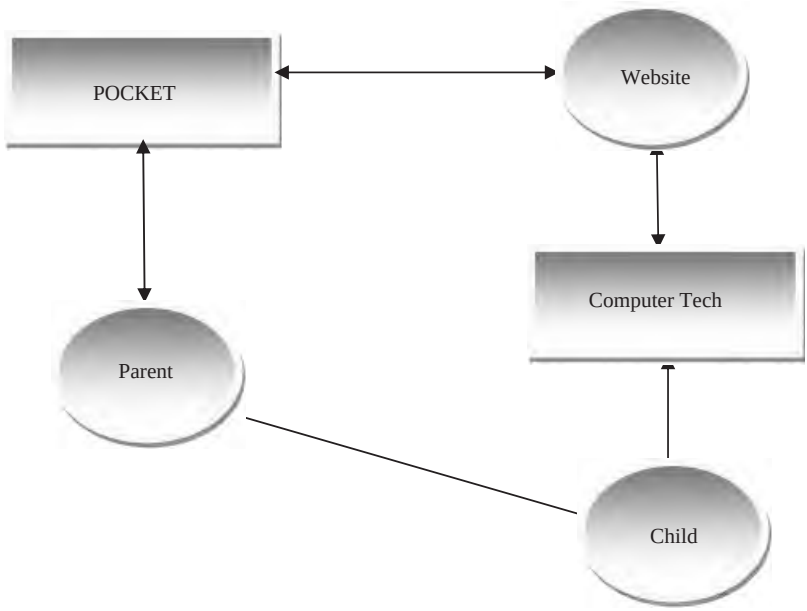


Figure 4. Robust POCKET-Aided Consent

As noted by the FTC, falsification of age by children is a problem that needs attention. Although the conceptual POCKET system does not address the issue directly, it is an example of an effective approach. Because the child's computer queries the Web site with POCKET, it indirectly communicates that a child under the age of thirteen is seeking to visit that site. Thus, the thorny problem of how to prevent a child from circumventing age verification procedures is solved by giving parents a method for signaling that the Web site visitor is a young child. POCKET's password system prevents the child from circumventing the technology of control.[175]

Lastly, identification of a parent, for purposes of consent, is important. Although POCKET does not incorporate a particular form of identification technology, it is designed to utilize a more secure method of identification upon the parent's registration. The present methods used by

[175]Many Web sites use cookies to prevent the child from reentering a site and trying to register at an older age. Children are adept at knowing how to clear the cookies file and circumventing this basic technology. Similarly, sometimes the age identification process can be fooled by simply reloading the Web page.

most Web sites are rather simplistic and do not rely on sophisticated methods of identification. In fact, it would be cost prohibitive to require these methods of identification for every time a child visited each individual Web site. POCKET allows for a more sophisticated method of identification to be used once, when the parent registers, and from that time forward the parent's choices are implemented by the software. Future changes are instituted only with the parent's password. No individual Web site is required to obtain direct parental identification. This accomplishes two goals: it implements a more secure parental consent mechanism and it is cost efficient for the Web site.

POCKET helps a parent to limit information sharing by a child by automating the decision and consent process. It gives a parent a way to be technically present when he or she is unable to be physically present. In sum, this proof of concept shows that presently available technology *can* be implemented to achieve a strong parental consent mechanism and to protect children.

E. Possible Approaches to Strengthening COPPA

The history of the adoption of COPPA, and the subsequent regulatory review of parental consent mechanisms, contains evidence of compromise and a deference to market mechanisms. From the beginning, the Senate cosponsor of the bill described the process as "consensus" building and noted the "participation of the marketing and online industries, the Federal Trade Commission, privacy groups, and First Amendment organizations."[176] The consensus led to the first constitutional privacy protection law for children online, and to changes in Web site operation that gave notice to parents and limited information collection from children. These accomplishments are significant and should not be minimized. Subsequent years without progress toward a technical solution for protecting children, however, reveal the inherent weakness in COPPA's lack of standards. Senator Bryan unsuccessfully proposed privacy legislation at the same time as COPPA, describing the approach: "[If] technological tools don't exist, or where a particular industry refuses to embrace this code . . . then the gov-

---

[176]*See* 144 Cong. Rec. S12741-04 (1998) (remarks of Sen. Bryan introducing the Senate version of the bill).

ernment is obliged to step in and reinforce protection of privacy rights."[177] The POCKET proof of concept shows that presently available technology exists to help parents protect their children's personal information, however, market incentives to implement technology improvements are lacking. As we approach a decade of study, legislation, and regulations to protect children's privacy, it may be time to address these technical failures with renewed regulatory guidance.

The FTC applies a test of reasonableness to whether a technical system should be required for obtaining parental consent; in order to be required, the system must be widely available and cost efficient.[178] If the FTC continues to rely only on the private sector to develop technology that meets this test, it is unlikely that there will be progress toward a technical solution, in part because there is no incentive for businesses to develop a technology while the FTC continues to accept the minimalist sliding-scale approach. Under the present regulatory regime, only FTC enforcement actions provide an incentive for businesses to develop a more sophisticated technical means of compliance. While businesses incur an economic risk by violating the regulations, as illustrated by the $1 million fine against Xanga, the risk is minimized because the FTC has limited resources to monitor Web sites for compliance, and parents have no individual right of action for a violation of the law. The Xanga site violations, although eventually uncovered, occurred over a five-year period. This case of delayed discovery illustrates that enforcement is significantly limited, and therefore, consequently, the incentive for business to adopt new technology is weak.[179]

The FTC should consider multiple, additional methods for spurring the adoption of technology to protect children online. Regulations that utilize technology to protect consumers, or gain efficiency, already exist in

---

[177] *Id.*

[178] Standardized technology would likely require a "massive educational effort . . . [and would need to be] compatible with most Internet sites, relatively easy for consumers to use, and difficult for data seekers to evade." *See* James P. Neff, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 60 (2003).

[179] It is worth considering whether parents, with a natural incentive to protect their children, might champion the development of the technology for their benefit. Although parents are more sophisticated and knowledgeable than their children in general matters, they are usually less proficient in the use of computers and technology. It is unlikely that parents could effect the change necessary for technical solutions. In fact, the potential adoptability of any technology will depend on an interface that is very easy for parents to use. *See* Crossler, *supra* note 169.

other technology-related areas. The FTC's do-not-call registry for phone solicitations is a successful example of a governmental, centrally operated solution. The majority of citizens have chosen to opt out of telephone solicitations[180] by joining a list that is maintained by the FTC.[181] A business must register with the National Do Not Call Registry, pay fees based on the number of area codes used, and download a list of telephone numbers from which it may not solicit by phone.[182] The business is free internally to choose the technology that will work best with the opt-out list. Other examples of government-supported technical solutions abound. Television broadcasters are required to provide closed captioning in order to provide access to viewers who are deaf.[183] In a more complex environment, individuals and businesses may file electronically with the Internal Revenue Service (IRS), through a system known as the Electronic Federal Tax Payment System.[184] The system for participating in the electronic filing is free and made available by the U.S. Treasury. More options for electronic payment are available through commercial software that may have additional enterprise benefits, but that software must meet technical standards established by the IRS.[185]

The FTC could make parental consent technology freely available or, in the example of POCKET, operate the server necessary for the process and allowing the business to design technology that will work best internally. Similarly, one or more safe harbor programs could also provide this service. However, the safe harbors do not have the same recognition by the public as the FTC, nor do they have the established consumer trust that made the FTC do-not-call regulation effective. The safe harbor programs do, however, have connections with children's Web sites and accountability

---

[180]*See* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 Notre Dame L. Rev. 583, 612 (2006).

[181]The FTC list can be found at the National Do Not Call Registry, *available at* https://telemarketing.donotcall.gov (last visited Mar. 27, 2008).

[182]The process is described on the "Create a Profile" page of the National Do Not Call Registry, https://telemarketing.donotcall.gov/profile/create.aspx (last visited Mar. 27, 2008).

[183]*See* Kesan & Shah, *supra* note 180, at 628–29.

[184]*See* Electronic Federal Tax Payment System, http://www.irs.gov/efile/article/0,,id=98005,00.html (last visited Mar. 27, 2008).

[185]The options available are listed on IRS e-file, http://www.irs.gov/efile/index.html (last visited Mar. 27, 2008).

mechanisms. A combination of FTC sponsorship or standard setting, and safe harbor requirements for business members, could prove to be the most effective and cost-efficient approach.

VI. Conclusion

Children are online at an increasingly young age, and they are subject to increasing dangers because of the evolving online environment of interactivity and social networking. MySpace exceeded the page views of Google and eBay years ago, and the AMA advises doctors to warn parents about potential Internet dangers.[186] Although the Internet brings rich content to children and expands their horizons, at the same time it also creates dangers and risks to their privacy and well-being. For the better part of a decade, the FTC championed the protection of children's privacy online. The FTC predicted since its COPPA regulations in 2000 that technology would provide the answer to protecting children online, yet no technology solution emerged. Clearly, Internet and communications technology have progressed rapidly and significantly in over seven years, yet protection of children's privacy seems to have been left behind. The goals of COPPA, to encourage the participation of parents in the online activities and decisions of their children and to facilitate the method of obtaining verifiable parental consent, can be accomplished with the aid of presently available technology, as illustrated by the POCKET proof of concept. POCKET shows that technology can empower parents to protect their children, yet incentives are lacking for businesses to develop similar, commercially available technology. Revised regulations could provide the incentives needed to spur the market to develop technology to protect children, technology that seemed so near when COPPA was initially adopted. Millions of children are online every day; protecting the richness of that experience while providing for the safety of their interaction is a parental goal that should be supported by the intersection of effective regulation and available technology.

---

[186] *See supra* note 12.

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.

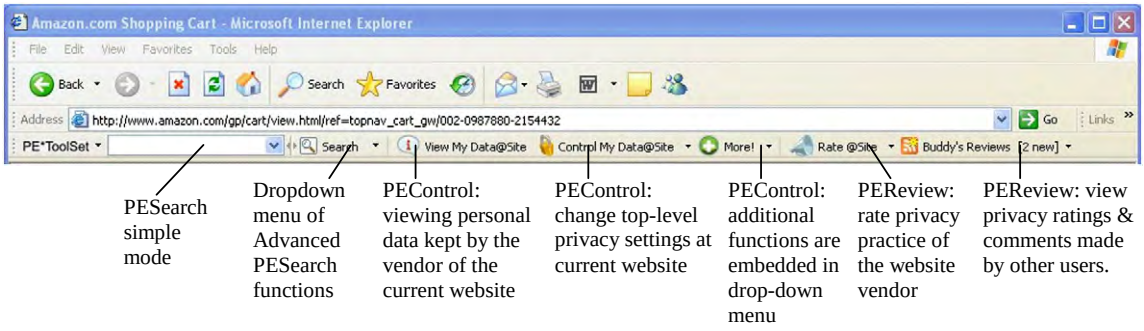


Fig. 1. The current design of the PE*ToolSet toolbar.

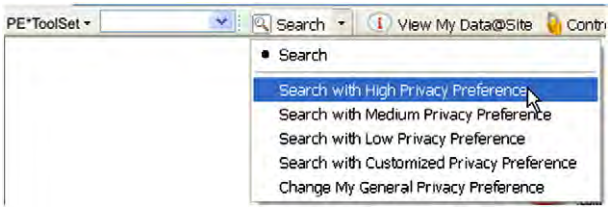


Fig. 3. Advanced PESearch functions in *Search!* dropdown menu.

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).

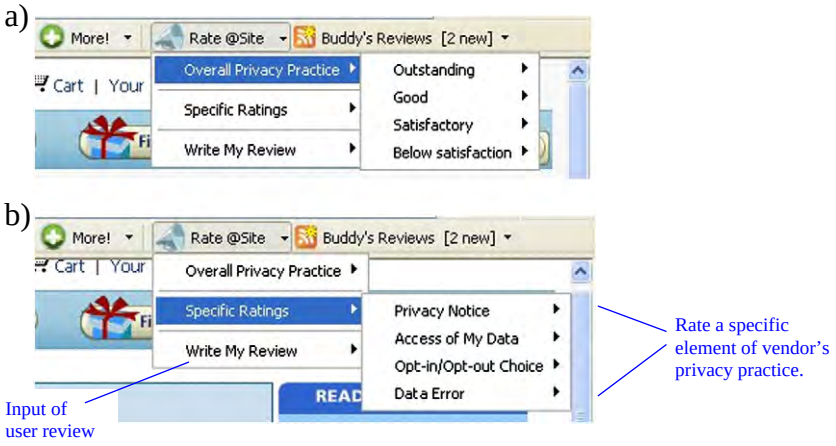


Fig. 4. a) Overall user rating on privacy practice in PEReview. b) Specific user rating and input of user review in PEReview.

"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].

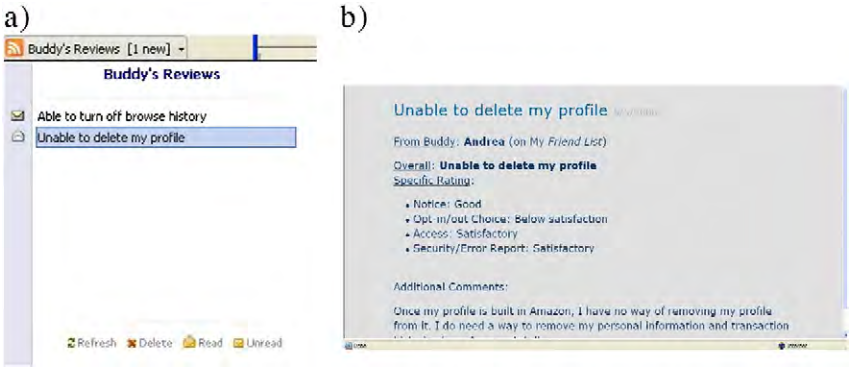


Fig. 5. a) Summary view of buddy's privacy review in PEReview. b) Detailed view of a buddy's privacy review in PEReview.

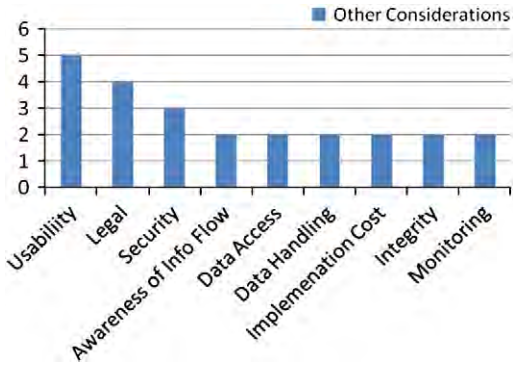


Fig. 6. Technical evaluation: expert suggestions for improvements.

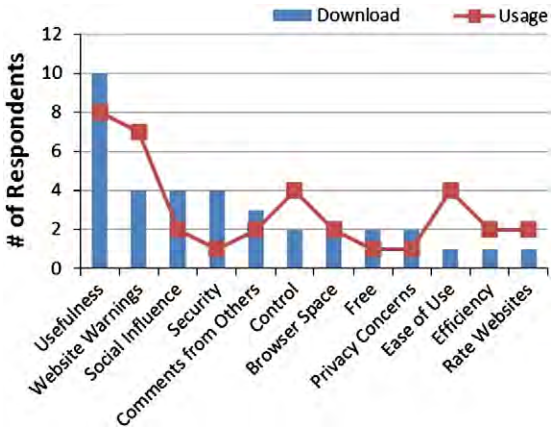


Fig. 7. Technical evaluation: novice.

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).