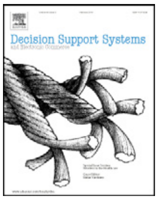
Decision Support Systems 54 (2013) 1161–1173

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

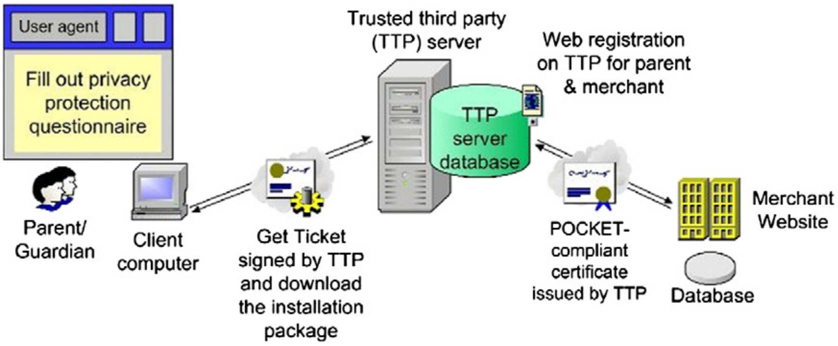

User agent
Fill out privacy protection questionnaire
Parent/ Guardian
Client computer
Get Ticket signed by TTP and download the installation package
Trusted third party (TTP) server
TTP server database
Web registration on TTP for parent & merchant
POCKET-compliant certificate issued by TTP
Merchant Website
Database

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

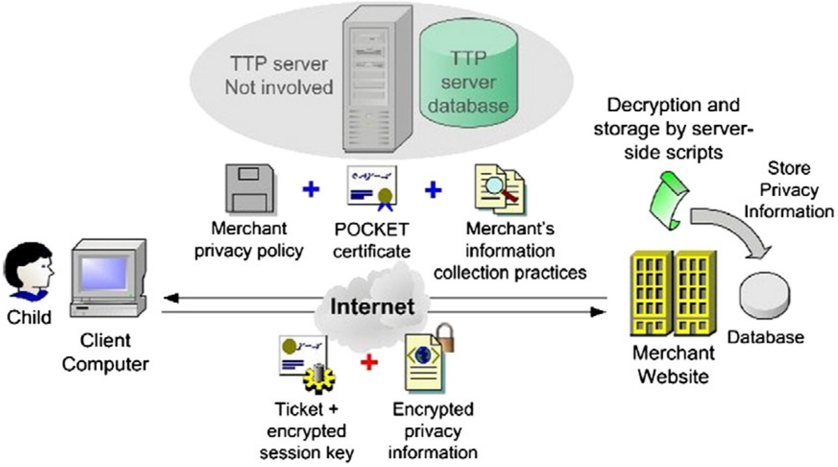


Fig. 2. POCKET transaction phase.

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.

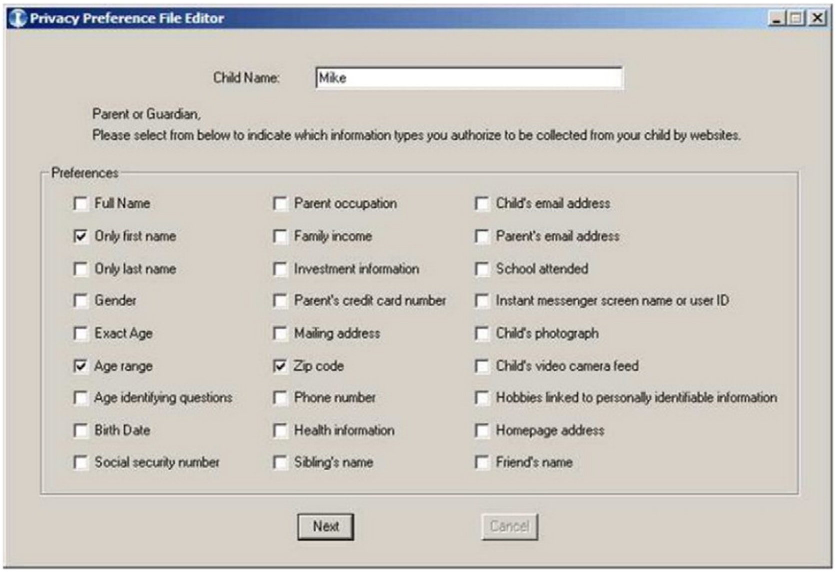
The man-in-the-middle attack is another type of attack that can be launched against this system. This attack happens when a valid packet is intercepted and manipulated or processed for information. Potential problems with a man-in-the-middle attack are (1) eavesdropping on sensitive and personal information, (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.



Child Name: Mike

Parent or Guardian,
Please select from below to indicate which information types you authorize to be collected from your child by websites.

Preferences

□ Full Name
☑ Only first name
□ Only last name
□ Gender
□ Exact Age
☑ Age range
□ Age identifying questions
□ Birth Date
□ Social security number
□ Parent occupation
□ Family income
□ Investment information
□ Parent's credit card number
□ Mailing address
☑ Zip code
□ Phone number
□ Health information
□ Sibling's name
□ Child's email address
□ Parent's email address
□ School attended
□ Instant messenger screen name or user ID
□ Child's photograph
□ Child's video camera feed
□ Hobbies linked to personally identifiable information
□ Homepage address
□ Friend's name

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

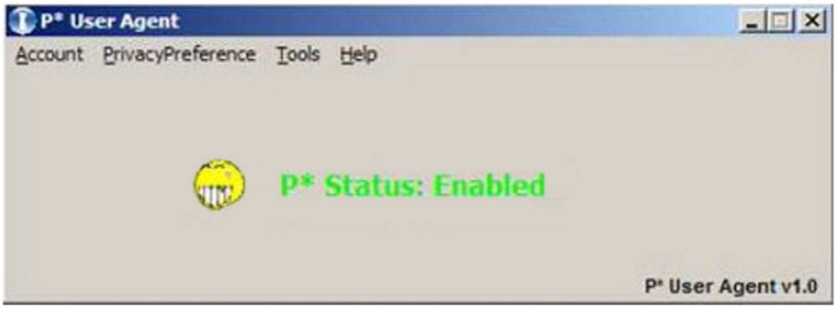
POCKET is designed to be a technical advancement of the requirements of COPPA, without displacing or becoming a safe harbor program. In essence, it will strengthen the protection of children by offering a more robust method for implementing COPPA and subsequent FTC regulatory requirements. Therefore, 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.

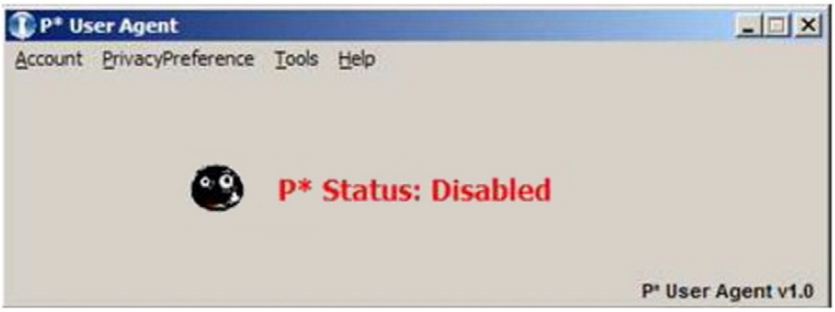
Black box testing involves the selection of different inputs at the user interface. It allows the tester to concentrate on hard-to-reach paths in other forms of testing and also helps to assure a high degree of reliability in the operation of the entire system. For POCKET, we



P* Status: Enabled

P* User Agent v1.0

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



P* Status: Disabled

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 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.

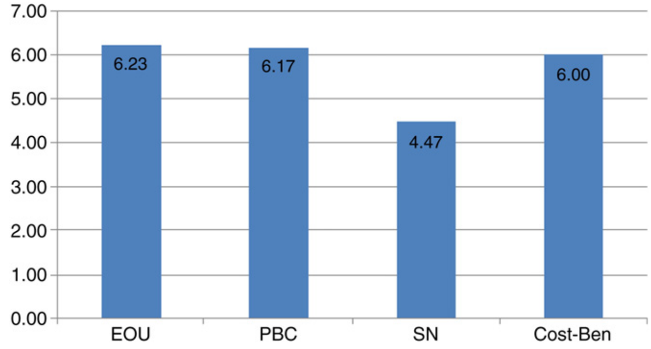


Fig. 6. Comparison of means for behavioral evaluation measures.

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.