

محافظت از حریم خصوصی بر خط کودکان به همراه رضایت هم‌زمان والدین آن‌ها برای تراکنش‌های الکترونیکی

حجت حمیدی^۱

تاریخ دریافت: ۹۴/۰۳/۲۰

تاریخ پذیرش: ۹۴/۰۵/۳۱

چکیده

یکی از بزرگ‌ترین نگرانی‌های کاربران اینترنتی، محافظت از حریم خصوصی‌شان است. با توجه به آمار و ارقام بالای استفاده از شبکه‌های اجتماعی بر خط، پتانسیل سوءاستفاده بر خط از کودکان افزایش یافته است. رضایت بر خط والدین برای تراکنش‌های الکترونیکی کودکان (POCKET)، یک نمونه برای برآورده نمودن الزامات قوانین محافظت از حریم خصوصی کودکان فراهم می‌کند. این مقاله، ابزاری خودکار، به نام رضایت والدین را برای تراکنش‌های الکترونیکی کودکان به منظور حفظ حریم خصوصی بر خط آن‌ها، ارائه می‌دهد. رضایت بر خط والدین رویکردی برای اجرای خودکار محافظت از حریم خصوصی بر خط کودکان، می‌باشد. تحقیقات، بررسی‌های بیشتری از حریم خصوصی بر خط کودکان را نشان می‌دهد که شامل شناسایی معیارهای تأثیرگذار بر استفاده والدین از نرم‌افزار به منظور محافظت از حریم خصوصی فرزند آن‌ها و توضیحی از نیازهای والدین برای محافظت از این حریم می‌باشد. نتایج ارزیابی تمام معیارهایی که می‌توان از طریق توسعه رضایت بر خط والدین برای تراکنش‌های الکترونیکی کودکان کنترل نمود نشان می‌دهد که والدین بر این عقیده‌اند که POCKET، انتظارات آن‌ها را برآورده می‌کند. ساختار هنجار اجتماعی که نمی‌تواند در توسعه POCKET کنترل شود نیز بالاتر از نقطه میانی مقیاس بوده است که نشان می‌دهد هرچند این عامل مهم‌ترین آئیم در تعیین ظرفیت استفاده والدین از POCKET نیست، ولی آنچه دیگر والدین انجام می‌دهند، برای تمایل به استفاده آن‌ها از POCKET مهم می‌باشد.

کلید واژه‌ها: حریم خصوصی، حفظ حریم خصوصی بر خط کودکان، شبکه‌های اجتماعی بر خط، POCKET^۲

۱- استادیار گروه فناوری اطلاعات - دانشگاه صنعتی خواجه نصیرالدین طوسی تهران، h_hamidi@kntu.ac.ir

2. Parental Online Consent for Kid's Electronic Transactions

۱- مقدمه

شبکه‌های اجتماعی بر خط آزادی زیادی به کاربران می‌دهند که برخی از کاربران می‌توانند از آن سوءاستفاده کنند. چنین مواردی با پایان‌های ناخوشایندی مانند خودکشی به خصوص در میان کودکان و جوانان به‌وفور دیده می‌شود. مزاحمت سایبری و آزار و اذیت سایبری منجر به آسیب‌های روحی برای قربانیان می‌شود (Schneider, Corley, Irons, 1998). مزاحمت سایبری به عنوان استفاده از خدمات اینترنتی و فناوری موبایل از قبیل صفحات وب، گروه‌های بحث و گفتگو، پیام فوری یا سرویس پیام کوتاه با هدف صدمه زدن به دیگران تعریف می‌شود. از سوی دیگر آزار و اذیت سایبری با عنوان استفاده از اینترنت یا سایر وسایل الکترونیکی برای آزردن فرد یا افراد دیگر یا یک سازمان تعریف می‌شود. آزار و اذیت اینترنتی ممکن است شامل اتهامات، نظارت، تهدید، سرقت هویت، تخریب داده‌ها و تجهیزات، درخواست‌های جنسی از افراد یا جمع‌آوری اطلاعات برای آزار سایرین، می‌باشد. به دلیل خصوصیت حضور از راه دور فضای سایبری، گمنامی و عدم وجود یک قدرت مرکزی، محدودیتی برای پست‌های اعضای شبکه‌های اجتماعی وجود ندارد. بنابراین افراد تصور می‌کنند اجازه دارند اظهارات زشت و متعارضانه، یا تصاویری را که تأثیر زیادی بر احساسات اعضای شبکه اجتماعی دارند و می‌توانند منجر به خودکشی نوجوانان و جوانان شوند، در شبکه اجتماعی به اشتراک بگذارند. آمارها نشان می‌دهد آزار و اذیت سایبری یک مشکل جدی به خصوص در میان کودکان است. (Livingstone, Helsper, 2008). با توجه به آمار اذیت‌های سایبری:

- بیش از نیمی از کودکان به صورت بر خط مورد آزار و اذیت قرار گرفته‌اند و بسیاری از آن‌ها در آزار و اذیت‌های اینترنتی شرکت داشته‌اند.
 - بیش از یک‌سوم کودکان تهدیدهای بر خط را تجربه کرده‌اند.
 - بیش از ۲۵٪ کودکان به‌طور مکرر از طریق تلفن‌های شخصی خود یا اینترنت مورد آزار و اذیت قرار گرفته‌اند.
 - بیش از نیمی از کودکان آزار و اذیت‌های سایبری را با والدین خود در میان نمی‌گذارند.
- همان‌طور که آمارها نشان می‌دهد، تعداد خودکشی‌های کودکان به دلیل آزار و اذیت‌های سایبری رو به افزایش است.

POCKET بدین منظور طراحی شده تا اجازه کنترل دسترسی‌ها را به والدین بدهد مگر این‌که وب‌سایت موافقت کند که پارامترهای جمع‌آوری اطلاعات توسط والدین تنظیم گردد. POCKET واسطه ساده‌ای برای والدین فراهم می‌کند تا تصمیمات حریم خصوصی فرزندشان را شکل دهند و سپس به

صورت خودکار این سیاست‌ها را اجرا نماید. برنامه POCKET با ثبت تعاملات صورت گرفته با وبسایت‌ها، در موارد اختلاف، راهی برای کسب اطمینان از قابل اعتماد بودن یک وبسایت را فراهم می‌کند. در این تحقیق نتایج قابل توجهی به دست آمده است. این تحقیق جنبه‌های مختلفی را در نظر گرفته است. اول به صورت منحصربه‌فردی مسائل نظری و فنی قانون تجاری، مهندسی کامپیوتر، و سیستم‌های اطلاعاتی ترکیب شده‌اند تا ابزاری ایجاد گردد که جواب‌گویی و اجرای قوانین را فراهم نماید. ما از طریق تبیین نظریه‌های اساسی که به طور ضمنی با POCKET در هم آمیخته است، زمینه را برای انطباق گسترده‌تر با قوانین در آینده و دیگر فعالیت‌های منظم اینترنت فراهم می‌کنیم. دوم، POCKET کاربر روی P3P (واسطی برای پروژه حریم خصوصی) را توسعه می‌دهد. سوم، تحقیقات، بررسی‌های بیشتری از حریم خصوصی بر خط کودکان را نشان می‌دهد که شامل شناسایی عوامل تأثیرگذار بر استفاده والدین از نرم‌افزار به منظور محافظت از حریم خصوصی بر خط کودکان و توضیحی از نیازهای والدین برای محافظت از حریم خصوصی بر خط کودکان می‌باشد. چهارم، طراحی نشان می‌دهد که چگونه محققان باید برای والدینی که چندان با فناوری آشنا نیستند راه‌حل‌های قابل استفاده‌ای ارائه دهند. در نهایت، مقاله نشان می‌دهد که چگونه علم طراحی می‌تواند به منظور فراهم کردن ابزاری مناسب و سودمند برای اشخاص مورد استفاده قرار گیرد و گام مشخصی در باب حریم خصوصی بردارد.

حریم خصوصی شامل مجموعه‌ای از حقوق انسانی مانند حق خلوت، یعنی حق تنها ماندن بدون مزاحمت دیگران، حق گمنامی، یعنی حق عمومی نکردن هویت شخصی، حق تحت نظارت قرار نگرفتن و حق حفاظت از اطلاعات شخصی می‌باشد (Bélanger, 2012). انسان‌ها ارزش زیادی برای این حقوق قائل هستند. درواقع، این حقوق بخشی از سیستم اخلاقی و معنوی هستند. با ظهور اینترنت و با افزایش ارزش اطلاعات، حریم خصوصی نیز ارزش بیشتری یافته است. ارزش حریم خصوصی به دلیل نقش آن در حفاظت از هویت شخصی افراد و گمنامی افراد است. هرچه اطلاعات کم‌تری از افراد در اختیار دیگران قرار گیرد، افراد احساس گمنامی بیشتری خواهند داشت. اگرچه افراد با توجه به مقدار، کیفیت و ارزش اطلاعاتی که از سایرین دارند، گمنامی آن‌ها را به چالش می‌کشند. مردم معمولاً تمایل دارند با افراد و گروه‌هایی ارتباط برقرار کنند که گمنامی آن‌ها را محترم بشمارند. هرچه اطلاعات ارزشمندتر و مهم‌تر باشند، اهمیت حفاظت از آن‌ها برای افراد افزایش می‌یابد. هویت شخصی یک منبع ارزشمند اطلاعات است. متأسفانه، با پیشرفت‌های سریع در فناوری، به خصوص در فناوری‌های ارتباطات راه دور، مراقبت و حفاظت از اطلاعات شخصی و هویت شخصی افراد بسیار مشکل‌تر شده است. هدف این تحقیق، تجزیه و تحلیل رویکردی

مبتنی بر رضایت بر خط والدین بر تبادلات الکترونیکی کودکان بوده که یک فناوری قابل اطمینان برای رضایت والدین می‌باشد.

۲- بیان مسئله

اجتماعات فیزیکی یک مرکز قدرت دارند که تمام اعضای اجتماعات بر خط باید از آن پیروی کنند. برخلاف اجتماعات فیزیکی، در اجتماعات بر خط شامل شبکه‌های اجتماعی بر خط هیچ قدرت مرکزی وجود ندارد و قدرت و مسئولیت‌پذیری برای تمام اعضا وجود دارد. این نوع اجتماعات بدون قدرت مرکزی و با قدرت و مسئولیت‌پذیری به اشتراک گذاشته شده، نسبتاً جدید هستند و نیازمند مکانیزمی است که از تمام اعضای اجتماع حفاظت کنند. اما چنین مکانیزم‌هایی هنوز تعریف نشده‌اند و در صورتی که تعریف شوند، برای قضاوت در مورد اثربخشی آن‌ها زمان لازم است.

توصیه نظارت کارهای کودکان به منظور حفاظت از آن‌ها در برابر خطرات احتمالی است، اما درعین حال اجازه بر خط بودن را نیز به کودکان می‌دهد. طبق بحث‌های علمی و عمومی، تهدیدهایی که کودکان با آن‌ها مواجه‌اند بسیار زیادند (Casilli, Tubaro, and Araya, 2012). در این بحث موارد بسیاری از اثرات منفی اینترنت روی کودکان مطرح شده است. نگرانی‌ها بیشتر روی محتوای مضر اینترنت، خطرات تعاملات بر خط و تهدیدهای بر خط حریم خصوصی متمرکز می‌شوند.

مضرات بالقوه محتوای بر خط شامل این موارد است: تجاری، خشونت، مسائل جنسی یا گفت‌وگوهای ضد اجتماعی مربوط به خردسالان، یا حرف‌هایی که مربوط به بزرگسالان است اما توسط خردسالان قابل دسترسی است. در حقیقت بعضی وبسایت‌ها ممکن است اطلاعاتی در رابطه با چگونگی انجام کارهایی نظیر خودکشی، آسیب رساندن به بقیه، تولید مواد مخدر، یا رفتارهایی مثل امتناع از غذا خوردن و اختلالات خورد و خوراک فراهم کنند. همان‌گونه که ما برای دستیابی به اطلاعات و سرگرمی از سایر منابع غیر اینترنتی روی گردانیم، به همین شکل تبلیغ‌کنندگان و افراد دارای منافع تجاری نیز به اینترنت روی آورده‌اند. امروزه مشتری‌مداری همراه با تصاویر و ارزش‌های شرکت‌های بسیار در اینترنت نفوذ کرده است. در حقیقت شرکت‌ها محتواهای کاملاً بر خطی ایجاد کرده‌اند که در تحقیقات تجاری روی خردسالان به کار گرفته شوند تا به منظور تبلیغات مؤثرتر برای آن‌ها اطلاعات شخصی‌شان را جمع‌آوری کنند.

همان‌گونه که هیچ‌کس نمی‌خواهد در معرض تبلیغات سوء، ناخواسته، و یا سخن‌رانی‌های توهین‌آمیز قرار گیرد، این استدلال مطرح می‌شود که افراد زیر سن قانونی بیشتر از بزرگسالان نسبت به این مسائل

آسیب‌پذیرند. به عنوان مثال، در یک مورد برجسته، کمیسیون ارتباطات فدرال کمیسیون ارتباطات، در ایالت کالیفرنیا، دیوان عالی ایالات متحده آمریکا اعلام نمود که: کودکان قادر نیستند از خود در برابر سخنانی که برای اکثر بزرگسالان تکان‌دهنده است، و به طور کلی، در صورت عدم علاقه به انتخاب خود از آن اجتناب می‌کنند، از خود محافظت کنند (Bélanger, Crossler, 2011). در عین حال، چنین سخنانی ممکن است اثرات منفی عمیق‌تر و بادوام‌تری روی یک کودک، نسبت به یک بزرگسال، بگذارد. بچه‌های کوچک‌تر ممکن است در برابر اثرات عاطفی تصاویر و اطلاعات حساس‌تر باشند. کودکان تجربه و توانایی شناخت کافی برای ارزیابی اطلاعات دریافتی را ندارند، به علاوه از کنترل انگیزشی کم‌تری برخوردار هستند و بنابراین تمایل دارند نسبت به اطلاعات دریافتی عکس‌العمل بیشتری نشان دهند.

نگرانی بیشتر درباره مواجهه شدن کودک با آسیب‌های احتمالی هنگام برقراری ارتباط بر خط با دیگران است. گزارش‌های نگران‌کننده مکرری درباره «شکارچیان اینترنتی» وجود دارد. که ممکن است ابتدا به صورت بر خط ارتباط را با خردسالان آغاز کنند، از آن‌ها درخواست عکس نمایند یا دست به ارتباطات نادرستی بزنند و شاید بچه را متقاعد کنند که فرد را ببیند از جمله این گزارش‌هاست. همان‌طور که یک مادر نگران اقرار کرده است، "هنگامی که دخترم لپ‌تاپش را روشن می‌کند... کل دنیا می‌تواند به آن دسترسی داشته باشند - هر غریبه‌ای می‌تواند وارد آن شود". هرچند که این نمونه تهدیدها بسیار جدی هستند اما مطالعات نشان می‌دهد که این خطرات معمولاً اغراق‌آمیزند. گذاشتن نظرات مربوط به روابط جنسی و دادن چنین پیشنهادهایی به همدیگر بین جوانان بسیار رایج شده است. این که اکثر تعاملات بر خط به صورت دوستانه هستند، همه آن‌ها را بی‌ضرر نمی‌کند. به خاطر طبیعت تعاملی همه مضرات یا خطرات رفتاری که به صورت آفلاین بین خردسالان اتفاق می‌افتد هم‌اکنون می‌تواند به صورت بر خط نیز رخ دهد مثل قلدری کردن، شایعه‌پراکنی، بردن آبروی افراد، اذیت کردن، ترغیب همدیگر به خطر جویی (در مسائل جنسی یا غیره). به راستی، بسیاری افراد آزار و اذیت‌های کودکان در اینترنت را اولین تهدید برای کودکان بر خط به شمار می‌آورند (Cranor, 2003).

در نهایت، تهدیدهایی برای حریم خصوصی بر خط کودکان وجود دارد. تفاوت بین دنیای بر خط و آفلاین، ارتباطات بر خط کودکان را نسبت به تهاجم به حریم خصوصی یا آشکارسازی غیر عمد اطلاعات حساسشان، آسیب‌پذیر می‌کند. danah boyd در سال ۲۰۰۷، در این باره بیان می‌کند که شبکه‌های اجتماعی ویژگی‌هایی دارند که آن‌ها را نسبت به ارتباط آفلاین تهدیدآمیزتر می‌نماید. مسئله قابل ملاحظه این است که برخلاف صحبت کردن رودررو یا از طریق تلفن با یک دوست، ارتباطات بر خط ضبط

می‌شوند. بنابراین ماندگار، قابل جست‌وجو و قابل کپی‌برداری هستند. به علاوه ما روی دسترسی به این ارتباطات کنترل بسیار کم‌تری داریم. این ویژگی‌های ارتباطات بر خط، آن‌ها را به تهدیدات شدیدی برای حریم خصوصی تبدیل کرده است. برخلاف اشتراک اطلاعات در فضای حقیقی که معمولاً در طول زمان فراموش می‌شوند، در اینترنت، چنین اطلاعاتی به صورت بالقوه همیشه برای همه در دسترس‌اند. همان‌طور که Marwick در سال ۲۰۰۸، اشاره کرد با دیجیتالی شدن، اطلاعات عملاً غیرقابل استرداد می‌شوند و ممکن است توسط موجودیت‌های تجاری، دولت یا اشخاص برای اهداف تجاری یا دیگر اهداف نادرستی خریداری شوند. تهدیدات حریم خصوصی ارتباطات بر خط همه را تحت تأثیر قرار می‌دهد، به ویژه بچه‌ها بسیار آسیب‌پذیرند زیرا ممکن است آگاهی کم‌تری نسبت به این موضوع داشته باشند که چه اطلاعاتی شخصی است و عواقب احتمالی انتشار این اطلاعات را نیز ندانند. به علاوه، اطلاعات شخصی که بچه‌ها در کودکی به صورت بر خط منتشر می‌کنند ممکن است در بزرگسالی اثرات جدی روی زندگی آن‌ها بگذارد.

۳- روش کار

طراحی POCKET مستلزم سه گروه از افراد ذی‌نفع است: والدین، تاجر صاحب وبسایت، و شخص ثالث مورد اعتماد. با این حال، ارزیابی کاربر از POCKET، فقط والدین و وبسایت‌های تجاری را هدف قرار می‌دهد، چرا که آن‌ها تنها بازیکنان درگیر در فاز تراکنش POCKET هستند. نقش شخص ثالث مورد اعتماد، در اختیار داشتن گواهی‌هایی برای تأیید وبسایت‌های تجاری است، شبیه به نقش VerisignTM به عنوان ارائه‌دهنده گواهی امنیتی. به منظور بررسی POCKET از دیدگاه یک پدر و مادر، ما یک نظرسنجی بر خط از والدین دارای کودک زیر ۱۳ سال انجام دادیم. ابتدا، بعد از پاسخ دادن به سؤالات عمومی جمعیت شناختی، والدین دمویی (نسخه آزمایشی) از نمونه اولیه نرم‌افزار POCKET را مشاهده نمودند. سپس از آن‌ها سؤالاتی پرسیدیم تا اطمینان حاصل کنیم که در طراحی POCKET شرایط خاصی که والدین در مرحله گروه‌های متمرکز ارائه نمودند، رعایت شده است. به‌طور خاص ما بر اندازه‌گیری سهولت استفاده (Venkatesh, Morris, Davis, 2014)، درک کنترل رفتاری (Taylor, Todd, 2014)، و هزینه - منفعت POCKET متمرکز شدیم (شکل ۱). هم‌چنین تأثیر هنجارهای اجتماعی (Venkatesh, Morris, Davis, 2014)، بر استفاده از این نرم‌افزار را نیز اندازه‌گیری نمودیم، چرا که این عامل از گروه‌های متمرکز بر خواسته بود، اما جزء رفتاری نبود که بتوان در طراحی POCKET آن را کنترل نمود. ارزیابی‌شوندگان با استفاده از یک نمونه ساده از والدین کودکان زیر سن ۱۳ سال در مناطق جغرافیایی مختلف انتخاب شدند.

نویسندگان با پدر و مادری که از این تحقیق مطلع نبودند، تماس گرفتند و لینی از این نظرسنجی را در اختیار آن‌ها قرار دادند. برای تشویق آن‌ها به شرکت در نظرسنجی، از طریق یک قرعه‌کشی جوایز کوچکی به شرکت‌کنندگان داده شد. در ایمیل‌های ارسالی به والدین از آن‌ها درخواست شده بود تا لینی نظرسنجی را به پدر و مادری که می‌شناسند و دارای کودک زیر ۱۳ سال هستند، نیز ارسال کنند. به منظور اعتبارسنجی، و با توجه به سؤالات محدودی که در پرسشنامه گنجانده شده بود، پاسخ ۱۰۵ کاربر را هدف قرار دادیم. ۱۰۵ پاسخ دریافت نمودیم و بعد از آن پاسخ‌نامه‌های دارای پرسش بدون پاسخ را جدا کردیم، ۱۵ امتیاز داده‌ای داشتیم تا میزان رعایت الزامات رفتاری را مورد ارزیابی قرار دهیم. پاسخ‌دهندگان به‌طور متوسط ۴۲/۸ سال سن داشتند ۸۷٪ مرد و ۶۰٪ زن بودند. پاسخ‌دهندگان ابراز نمودند که متوسط زمان بر خط بودن فرزندان (زیر سن ۱۳ سال) آن‌ها ۴/۳ ساعت در هفته است. قبل از ارزیابی پاسخ‌های شرایط رفتاری، قابلیت اطمینان و اعتبار ابزارهای استفاده‌شده را مورد آزمایش قرار دادیم. همه سازه‌های دارای بیش از یک آیتم، دارای آلفا کرونباخ بالاتر از ۰/۷۰، بودند و این نشان‌دهنده قابلیت اعتماد معیارها بود. اعتبار سازه با استفاده از یک تحلیل عاملی تأییدی مورد آزمایش قرار گرفت، و هیچ سؤالی دارای مشکل بارگذاری نبود. برای ارزیابی POCKET، هدف ما این بود اطمینان حاصل کنیم که این ابزار، شرایط از پیش تعریف‌شده را که از گروه متمرکز برآمده بود، برآورده نموده است. به این ترتیب، متوسط هر معیار به جز در مورد هزینه - منفعت، که فقط یک آیتم داشت، محاسبه گردید. آیتم‌ها در طیفی شبیه طیف لیکرت از ۱ تا ۷ اندازه‌گیری شدند.

راه‌هایی برای افزایش امنیت بر خط بدون تجاوز به حریم خصوصی:

استدلال کردیم که والدین نباید تبادلات اطلاعاتی فرزندان را به خاطر محافظت آن‌ها از خطرات احتمالی بر خط، نظارت کنند، زیرا این کار تجاوز به حریم خصوصی کودک محسوب می‌شود. هنوز مشکلی که در ابتدای مقاله مطرح شد وجود دارد: چگونه می‌توانیم موجب لذت بردن فرزندان از مزایای شخصی، اجتماعی و آموزشی بر خط شویم و خطرات احتمالی آسیب رسیدن به آن‌ها از طریق محتواهای ناخواسته‌ای نظیر آزار و اذیت‌های اینترنتی یا درخواست‌های ارتباط جنسی ناخواسته را به حداقل برسانیم؟ برخی معتقدند که پاسخ این است که تنظیم دسترسی کودکان به اینترنت را از دست والدین خارج کرده و به قانون‌گذاران بسپاریم. برای مثال Livingstone Sonia و Magdalena Bober در سال ۲۰۰۶ و ۲۰۰۵ اظهار کردند که "به خاطر دلایل عملی و نظری"، کنترل فعالیت‌های اینترنتی خردسالان "سخت

است و مسئولیت بی‌جایی برای گذاشتن بر دوش والدین می‌باشد". والدین و فرزندان می‌توانند در مذاکرات دموکراتیک درباره قوانین دوجانبه، اعتماد و مسئولیت‌ها در خصوص استفاده از اینترنت شرکت کنند. مدل‌های بسیاری وجود دارد که چگونگی انجام چنین مذاکراتی را نشان می‌دهد. به نظر می‌آید استفاده از استراتژی‌هایی نظیر "استفاده اجتماعی مشترک" یا "میانجی‌گری تعاملی" به جای نظارت، تهدیدها را بیشتر کاهش داده و موجب می‌شود فرزندان توانایی بیشتری داشته باشند تا از عهده مشکلات تجربه‌های بر خطشان برآیند. این استراتژی‌ها کارهایی را به والدین پیشنهاد می‌دهد مثلاً درباره ساختار و محتوای اینترنت با فرزندشان صحبت کنند، فرزندان را به جست‌وجو در اینترنت ترغیب کنند، مواقعی که فرزندان بر خط هستند در کنار یا نزدیک آن‌ها بنشینند و فعالیت‌های بر خط را به اشتراک بگذارند. گرچه یک روش برای همه مناسب نیست، اما نشان داده شده که استفاده اجتماعی مشترک، صرف‌نظر از تفاوت در فرهنگ تربیتی فرزندان، تهدیدها را کاهش می‌دهد. به یقین گفت‌وگوهای تشویقی ضرر کم‌تری نسبت به نظارت دارد، هم‌چنین این امکان را می‌دهد که آسیب‌های مربوط به تجربه‌های منفی بر خط را کاهش دهد. گفت‌وگو با پدر و مادر روشی است که موجب می‌شود فرزندان از عهده تجربیات بر خط منفی خود برآیند. اگر والدین فضای بازی در مورد فعالیت‌های بر خط ایجاد کنند، احتمالاً فرزندان تمایل بیشتری دارند که درباره مشکلات خود با پدر و مادر صحبت کنند. همان‌طور که در بالا اشاره شد، نظارت موجب خراب شدن اعتماد می‌گردد، و در نتیجه به اشتراک اطلاعاتی داوطلبانه فرزندان نیز لطمه وارد می‌کند. (Ratnasingam, 2015).

اصول نظری برای طراحی رضایت بر خط والدین:

پروژه POCKET به خاطر نبود راه‌حل‌های مناسب فنی برای اجرای نیازمندی‌های حقوقی ایجاد شد. هرچند که برای طراحی POCKET تیم تحقیقاتی نه تنها باید نیازمندی‌های حقوقی را بررسی کند بلکه نیازمندی‌های رفتاری و فنی هم باید موردبررسی قرار گیرد. ما از طراحی چارچوب علمی که Kuechler و Vaishnavi در سال ۲۰۱۲، ارائه دادند استفاده کردیم و بحث‌های نظریه‌های پایه، نیازمندی‌ها و اصول طراحی را مطابق با ساختار پیشنهادی توسط Ngai ارائه دادیم. چارچوب Kuechler و Vaishnavi نشان می‌دهد که چگونه در توسعه یک محصول، نظریه تلویحاً در آن مدنظر قرار می‌گیرد، محصولی که تماماً حاصل پژوهش علمی طراحی است. بر اساس این چارچوب و دیگر آثار علم طراحی، ما توسعه محصول خود را با نظریه‌های هسته شروع می‌کنیم که موجب شناسایی الزامات POCKET و درنهایت منجر به اصول

طراحی می‌گردد که توسعه محصول ما را هدایت می‌کند. نظریه‌های اساسی از طریق سه رشته مرجع، توسعه POCKET را پیش می‌برند که عبارت‌اند از: حقوق، علوم کامپیوتر و سیستم‌های اطلاعاتی. در قسمت بعد، نظریه‌های اساسی، نیازمندی‌ها و اصول طراحی POCKET را بیشتر توضیح می‌دهیم.

نیازمندی‌های حقوقی و اصول طراحی حقوقی:

نیازمندی‌های حقوقی قوانین محافظت از حریم خصوصی بر خط کودکان شامل موارد زیر است:

- ۱- تذکری از شیوه جمع‌آوری اطلاعات از جمله شیوه استفاده و افشای آن را فراهم کند.
- ۲- قبل از جمع‌آوری، استفاده یا افشای اطلاعات، رضایت والدین را به دست آورد. والدین باید قادر به اعلام عدم رضایت نیز باشند.
- ۳- دسترسی به اطلاعات جمع‌آوری‌شده، حق حذف اطلاعات و توانایی جلوگیری از جمع‌آوری بیشتر اطلاعات را برای والدین آسان سازد. همچنین والدین باید قادر باشند رضایت خود را تغییر دهند یا رد کنند.
- ۴- کودک را از مشارکت در فعالیت‌های بر خطی که موجب افشای اطلاعات می‌گردد منع کنند، مگر این‌که از لحاظ منطقی ضروری باشد.

- ۵- از صحت و امنیت اطلاعات جمع‌آوری و یا ذخیره‌شده محافظت و نگهداری کنند.
- انواع اطلاعاتی که طبق قوانین محافظت از حریم خصوصی بر خط کودکان می‌توانند برای شناسایی فردی موردبررسی قرار گیرند شامل طیف گسترده‌ای از عناصر اطلاعاتی است.
- الزامات مشخص‌شده در بالا منجر به شناسایی اصول طراحی شد که به منظور اطمینان از این‌که محصول نهایی POCKET شرایط موردنیاز دستورات حقوقی را تأمین می‌کند، باید دنبال شود. اصول طراحی حاصل به شرح زیر است:

- ۱- POCKET باید راهی برای شناسایی روش‌های حریم خصوصی سایت فراهم کند.
- ۲- POCKET باید فرآیند رضایت والدین برای آشکارسازی و استفاده از اطلاعات فرزندشان را به صورت مرحله‌به‌مرحله طبق ترجیحات از پیش تعیین‌شده والدین، خودکار نماید.
- ۳- POCKET باید روشی برای پدر و مادر فراهم کند تا اطلاعاتی را که توسط سایت فراهم‌شده، مرور کنند و اگر نیاز به حذف اطلاعات باشد وبسایت را مطلع سازند.
- ۴- این الزامات حقوقی فراتر از کنترل محصولی همچون POCKET است و یک تصمیم رفتاری از تاجران وبسایت می‌باشد.

۵- POCKET باید از اطلاعاتش محافظت کرده و اطلاعات صحیحی به تاجران وبسایت که اطلاعات را از طرف والدین با آن‌ها به اشتراک می‌گذارد، ارائه دهد.

محیط و الزامات فنی:

نظریه‌هایی که شرایط فنی لازم را اطلاع می‌دهند به‌طور ضمنی در طراحی نرم‌افزار موجود گنجانده شده‌اند مثل کوکی‌ها، ناشناس سازها، کنترل‌های نرم‌افزاری، سیاست‌های حریم خصوصی و نشان‌ها. طی سالیان، محققان ابزارها و تکنیک‌های مختلفی ایجاد کرده‌اند که از حریم خصوصی بر خط مشتریان محافظت می‌کنند (Mont and Bramhall, 2014). اگرچه که به‌طور مستقیم به حریم خصوصی فرزندان مربوط نمی‌شوند اما هر یک از این فناوری‌ها تلاش می‌کنند به مسائل امنیتی موجود در اینترنت اشاره کنند. هرچند که این ابزارها به‌طور موفقیت‌آمیزی همه مسائل حریم خصوصی که قبلاً بحث شد را برطرف نمی‌نمایند، و هیچ‌یک از آن‌ها قادر نیستند شرایط لازم قوانین محافظت از حریم خصوصی بر خط کودکان را به‌طور کامل برطرف کنند.

الزامات فنی POCKET از ترکیبی از عوامل حقوقی استخراج شده (به‌عنوان مثال اطلاعات ایمن نیازمند انتقال رمزگذاری شده‌اند)، عوامل فنی متناسب با محیط کار (به‌عنوان مثال لزوم استفاده وبسایت از پروتکل‌های اینترنت) و عوامل فنی است که از راه‌حل‌های فنی امکان‌پذیر موجود استفاده می‌کند. (به‌عنوان مثال P3P اطلاعات سیاست حفظ حریم خصوصی را فراهم می‌کند که می‌تواند توسط POCKET مورد استفاده قرار گیرد).

با توجه به محیط کار، طراحی POCKET باید شرایط والدینی را که کاربران این سیستم‌ها هستند در نظر بگیرند. به عبارت دیگر، سیستم باید به‌آسانی قابل اجرا و استفاده باشد (شرط - ۱). علاوه بر این، POCKET باید پیش از هر چیز در یک محیط محبوب مانند اینترنت اکسپلورر توسعه داده شود، که به احتمال زیاد به‌طور گسترده‌تر استفاده می‌شود (شرط - ۲).

از لحاظ محیط کاری و برای دستیابی به راه‌حل عملی، POCKET نیازمند استفاده از کوکی‌ها و ناشناس سازها است تا در موارد ممکن، نهایت شفافیت و خودکاری را فراهم نماید و کار والدین را در استفاده از نرم‌افزار تسهیل کند (شرط - ۳). هم‌چنین POCKET نیازمند استفاده از فناوری‌های پیشین P3P است (شرط - ۴). بسیاری از عوامل کاربری P3P در طول فرآیند استانداردسازی P3P توسعه یافتند. با این حال، P3P در پیاده‌سازی دارای مشکلاتی است، تحقیقات نشان‌دهنده خطاهایی در اجرای سیاست‌ها، نقض

سیاست، و سیاست‌های ناقص است. این باعث شده است که محققان توصیه کنند که یک شخص ثالث مورد استفاده قرار گیرد تا رعایت مقررات و سیاست‌ها را تأیید کند. حتی اگر P3P را بتوان به گونه‌ای قابل اعتماد اجرا نمود، ساخت زبان حفظ حریم خصوصی به اندازه کافی سنجیده نیست که بتواند به انتخاب‌های خاص والدین در مورد اطلاعات دقیقی که یک وبسایت می‌تواند یا نمی‌تواند جمع‌آوری و یا به اشتراک بگذارد، رسیدگی کند. در نهایت و مهم‌تر از همه، P3P هیچ روشی برای اظهار رضایت والدین در مورد اطلاعات کودک ارائه نمی‌کند. با این وجود، POCKET می‌تواند از مفاهیم اولیه P3P استفاده کند و آن‌ها را بهبود بخشد. یکی از توسعه‌های فنی و نهایی برای تعیین الزامات POCKET استفاده از نوار ابزارهای کنترلی در نرم‌افزار قبل است که نشان‌دهنده لزوم کسب اطمینان از کنترل والدین بر ابزار مزبور می‌باشد (شرط-۵).

اصول طراحی فنی:

بر اساس مروری که در بالا بر روی نظریه‌های هسته‌ای، راه‌حل‌های موجود، و شرایط لازم صورت گرفت، تیم تحقیقاتی، مجموعه‌ای از اصول طراحی را برای توسعه طرح اولیه POCKET ایجاد کردند.

نیاز ۱: اجرا و استفاده از سیستم باید ساده باشد.

اصل طراحی ۱،۱: POCKET باید به سادگی قابل دانلود باشد.

اصل طراحی ۱،۲: نصب POCKET باید ساده باشد.

اصل طراحی ۱،۳: اینترنتی‌س کاربر باید گرافیکی بوده و با استفاده از آیتم‌های منو و جعبه‌های دیالوگ کاربر را به راحتی هدایت کند؛ فهم پیام‌های خطا نیز باید ساده باشد.

نیاز ۲: طرح اولیه باید برای محیط عمومی توسعه یابد.

اصل طراحی ۲،۱: POCKET باید در ابتدا با استفاده از شیء کمک‌کننده به مرورگر (BHO) برای اینترنت اکسپلورر توسعه یابد.

نیاز ۳: طرح اولیه POCKET باید به اندازه کافی شفاف و تا حد ممکن خودکار باشد.

اصل طراحی ۳،۱: مرحله انتقال [چه انتقال اطلاعات تأیید شده باشد چه نه] باید هنگام نصب و کار با POCKET شفاف باشد.

اصل طراحی ۳،۲: POCKET به انتقال مطمئن اطلاعات بین والدین، وبسایت و ماشین‌های شخص ثالث نیاز دارد.

نیاز ۴: POCKET به تکنولوژی P3P نیاز دارد.

اصل طراحی ۴,۱: POCKET باید با استفاده از مفهوم عامل کاربری P3P به صورت خودکار فایل ترجیحات حریم خصوصی خود را با فایل روش‌های حریم خصوصی مقایسه کند.

نیاز ۵: POCKET باید امکان کنترل ابزار را به والدین بدهد.

اصل طراحی ۵,۱: POCKET باید والدین را قادر سازد تا تنظیمات را به دلخواه تغییر دهند.

نیاز ۶: POCKET باید به صورت ساختاریافته و مرحله‌به‌مرحله توسعه داده شود.

اصل طراحی ۶,۱: POCKET باید شامل ۴ فاز باشد: ثبت نام، نصب، تراکنش و فاز پس تراکنش

محیط و نیازمندی‌های رفتاری:

محیط رفتاری به نیاز POCKET برای قابل استفاده بودن توسط والدین اشاره دارد (مثلاً کسانی که از لحاظ فنی چندان ماهر نیستند، کسانی که ممکن است نخواهند وقت چندانی برای یادگیری نرم‌افزار صرف کنند و...) و توسط مجموعه گسترده‌ای از نظریه‌های هسته‌ای گزارش شده است همچون مدل تطابق با تکنولوژی، نگرانی برای حریم خصوصی اطلاعات، و اعتماد. قبل از طراحی ابزار POCKET، ما یک مدل اولیه از آن را برای نشان دادن به کاربران بالقوه (والدین) ایجاد کردیم تا بازخورد عمیقی از نیازمندی‌های مربوط به استفاده از چنین ابزاری را دریافت کنیم. بدین منظور ما روی ۴ گروه از پدر و مادرهایی که حداقل یک بچه از سن ۴ تا ۱۳ سال داشتند تمرکز کردیم. گروه‌های تمرکز یافته رویکرد مطلوبی در درک یک دامنه پژوهشی فراهم می‌کنند که قبلاً در آن‌ها پژوهش‌های محدودی انجام شده است چرا که آن‌ها با ارائه اطلاعات پس‌زمینه‌ای بیشتر در مورد شرایط، به محققان اجازه می‌دهند که بررسی عمیق‌تری از موضوع موردعلاقه خود داشته باشند.

رویه گروه‌های تمرکز یافته:

پیش از هدایت گروه‌های تمرکز یافته، یک مدل اولیه ایجاد و تست شد و بارها تغییر یافت. برای انتخاب شرکت‌کنندگان ما با گروه‌های مذهبی، جوامع ورزشی و جوامع والدین-معلمی از نقاط مختلف جغرافیایی ارتباط برقرار کردیم. ۴ گروه تمرکز یافته بدین صورت بودند: یکی از پدر و مادرهای جامعه فوتبالی، یکی از والدین - معلم و ۲ تا از گروه‌های مذهبی از نقاط مختلف. در هر جلسه ۳ تا ۶ فرد حضور داشت و در مجموع ۱۸ نفر والدین حاضر شدند. در حین پرسش از گروه‌ها، والدین فرم رضایتی را امضا کردند، به سؤالات آماری جواب دادند و به سؤالات آن‌ها پاسخ داده شد. جدول ۱ آمار را نشان می‌دهد.

اصول طراحی رفتاری:

نیازمندی‌های جدول ۲ در اصول طراحی که در ادامه آورده شده، نتیجه شدند. قابل ذکر است که بعضی از اصولی که به‌عنوان اصول طراحی رفتاری مشخص شدند با اصول طراحی حقوقی و فنی هم‌پوشانی دارند.

۱- POCKET باید برای استفاده آسان باشد (نیازمندی‌های ۱ و ۲ و ۷).

۲- POCKET باید نیازمندی‌های حقوقی را تأمین نماید (نیازمندی ۳).

۳- POCKET باید برای استفاده والدین فایل‌های ثبت وقایع ایجاد کند (نیازمندی ۴).

۴- POCKET باید بر روی اطلاعاتی که توسط فرزندان آشکار می‌گردد کنترل بیشتری فراهم کنند (نیازمندی ۵ و ۸).

۵- POCKET باید بیش‌ترین بهره‌وری را با کم‌ترین هزینه فراهم کند (نیازمندی ۶ و ۱۱).

جدول ۳ خلاصه‌ای از اصول طراحی POCKET را بر اساس نظریه‌های پایه حقوقی، فنی و رفتاری و نیازمندی‌هایی که در این قسمت بحث شد نشان می‌دهد.

جدول ۱- آمار پاسخ‌گویان

میانگین	محدوده	آمارگیری (n=105)
۳۸,۶	۴۸-۲۹	سن (سال)
۱۶,۶	۲۶-۸	تجربه کاری (سال)
۱۶,۷	۲۷-۶	تجربه استفاده از کامپیوتر (سال)
۴	۱۰-۱	تعداد فرزند
۱,۶	۳-۰	تعداد کامپیوترهای خانه
تعداد	دسته‌بندی‌ها	
۳۹	مرد	جنسیت
۶۶	زن	
۳۸	دبیرستان	تحصیلات
۲۱	فوق دیپلم	
۲۳	لیسانس	
۲۳	تحصیلات تکمیلی	

جلسات ضبط‌شده، به فایل‌های متنی رونویسی شد و برای آنالیز داده‌ها به یک برنامه کامپیوتری مورد استفاده برای آنالیز داده‌ها (Atlas.ti) وارد شد. لیست اولیه‌ای از دسته‌بندی‌های گروه‌ها و دانش

حاصل از آن‌ها شکل گرفت. لیست بارها تجدیدنظر شد. هنگامی که تیم روی دسته‌بندی‌های لیست توافق کردند، دو نفر، جلسات را کد نویسی کردند. سپس کدنویس‌ها با یکی از محققان ملاقات کردند تا کدشان را مقایسه کنند و روی تفاوت‌ها بحث کنند تا زمانی که روی گروه‌ها، معانی و رویه‌های کد نویسی بعدی توافق نمایند. سپس کدنویس‌ها بقیه رونوشت‌ها را با الگوهای کد نویسی تجدیدنظر شده، کد کردند. کاپای کوهن ۷۵٫۱٪ و حاکی از یک مرحله رضایت‌بخش بود (ضریب کاپای کوهن یک معیار آماری برای ارزیابی است). سپس از برنامه کامپیوتری برای به دست آوردن نتایج جدول استفاده شد. والدین در گروه‌ها، از قوانین، ابزارها و مسئله حریم خصوصی در اینترنت آگاهی یافتند. به علاوه، فاکتورهایی را شرح دادند که موجب می‌شد شروع به استفاده از ابزارهایی برای محافظت از حریم خصوصی بر خط فرزندانشان کنند. این فاکتورها در جدول ۲ نشان داده شده‌اند که آن‌هایی که از لحاظ فنی عملی بودند، به عنوان نیازمندی‌های POCKET شناخته شده‌اند. (توسط # به آن‌ها اشاره شده است).

جدول ۲- فاکتورهای استفاده ← نیازمندی‌ها

والدین از ابزار محافظت از حریم خصوصی استفاده خواهند کرد اگر...	تعداد پاسخ‌ها	درصد
۱- ... نیاز به تلاش کمی داشته باشد. (استفاده آسان) #	۷۵	۴۳٪
۲- ... تغییر تنظیماتش راحت باشد. #	۲۸	۱۴٪
۳- ... موردنیاز است زیرا درواقع مقررات از فرزندشان محافظت می‌کنند. #	۳۶	۸٪
۴- ... فایل‌های ثبت وقایع در دسترس باشند. (اما بتوانند روشن یا خاموش شوند) #	۲۶	۸٪
۵- ... به آن‌ها کنترل بیشتری برای رضایت بر سایت‌های مورد بازدید فرزندشان بدهد. #	۱۶	۵٪
۶- ... برای استفاده کارآمد است (هزینه - سود) #	۱۷	۵٪
۷- ... امنیتی از سایت‌های از پیش تعیین شده فراهم کند (راحتی) #	۲۴	۵٪
۸- ... به آن‌ها کنترل بیشتری بر روی حریم خصوصی فرزندشان بدهد. #	۱۵	۳٪
۹- ... افراد دیگری که آن‌ها می‌شناسند هم از آن‌ها استفاده کنند.	۱۷	۳٪
۱۰- ... در مدرسه هم اجرا شود.	۱۹	۳٪
۱۱- ... قابل دانلود باشد. #	۲۸	۳٪
کل	۲۹۹	۱۰۰٪

فاکتورهایی که در طراحی POCKET نقش داشته‌اند.

۴- یافته‌های پژوهشی

یکی از جنبه‌های مهم طراحی یک محصول فناوری اطلاعات ارزیابی آن است. در مورد POCKET، سه دسته اصول طراحی مختلف وجود دارد که باید مورد ارزیابی قرار گیرند.

۱- ارزیابی حقوقی در صورتی تأیید می‌شود که POCKET به نیازمندی‌های حقوقی بپردازد.

۲- ارزیابی فنی در صورتی تأیید می‌شود که POCKET به عنوان یک ابزار فنی کار کند و عاری از خطا باشد.

۳- ارزیابی رفتاری در صورتی تأیید می‌شود که POCKET نیازمندی‌های کاربر را برطرف نماید.

POCKET طراحی شده است تا بدون تغییر یا تبدیل شدن به یک برنامه کنترل امن، به پیشرفت فنی الزامات قوانین حفاظت از حریم خصوصی بر خط کودکان، تبدیل شود. درواقع این برنامه با ارائه روش قوی‌تر برای اجرای قوانین حفاظت از حریم خصوصی بر خط کودکان، و به دنبال آن الزامات حقوقی، حمایت از کودکان را تقویت می‌کند. بنابراین، انتظار نمی‌رود که تمامی اصول طراحی برآورده شده باشند. در نمودار زیر عناصری که به صورت/یتالیک نشان داده شده‌اند، به عناصر ایمنی اشاره دارد که برای برآوردن تمامی شرایط نظارتی موردنیازند. همان‌طور که جدول ۴ نشان می‌دهد، POCKET طوری طراحی شده است تا الزامات حقوقی رضایت والدین را تقویت کند، و آن شامل روش‌های مهمی برای تغییرات بعدی در رضایت و کنترل کلی والدین است. هدف از طراحی POCKET بر اساس تعدادی از اصول طراحی، این بوده است تا اطمینان حاصل شود که POCKET با نظریه‌های هسته فراگیری اجرا می‌شود که قبل از توسعه آن شناسایی شده بودند. ارزیابی حاصل که در بالا ارائه شده، نشان می‌دهد که POCKET با موفقیت توانسته مشخصات خاص حقوقی را که توسط قوانین حفاظت از حریم خصوصی بر خط کودکان، تعیین شده به دست بیاورد.

ارزیابی فنی POCKET شامل چندین مرحله است. اول، تست دقیق نرم‌افزار قرار دارد. هدف اصلی از آزمایش نرم‌افزار POCKET این است که اطمینان حاصل شود هنگامی که مجموعه‌ای از ورودی‌ها به برنامه داده می‌شود، سیستم به شکل مشخصی کار می‌کند. علاوه بر این، سیستم نباید نتایج غیرمنتظره‌ای بدهد و به واسطه آن قابلیت اطمینان خود را تضعیف کند. هدف POCKET پدر و مادرانی است که باید مطمئن باشند که سیستم می‌تواند وبسایت‌ها را بر اساس اولویت‌های مشخص شده، مسدود/ قابل دسترسی گرداند. برای کسب اطمینان از درستی آن، ما سیستم را به‌طور گسترده مورد آزمایش قرار دادیم. روند

آزمایش شامل دو مرحله است: تست جعبه سیاه و تست جعبه سفید. تست جعبه سیاه شامل انتخاب ورودی‌های مختلف در رابط کاربری است و این امکان را به آزماینده می‌دهد تا در اشکال گوناگون تست، به مسیرهای دشوار تمرکز کند و همچنین کمک می‌کند تا به درجه بالایی از قابلیت اطمینان در عملکرد کل سیستم دست پیدا کنیم. در مورد POCKET، ما رابط کاربر و شیء کمک‌کننده به مرورگر را مورد آزمایش قرار دادیم. برای تست جعبه سیاه و سفید، تمامی مسیرهای ممکن در نرم‌افزار را مشخص کردیم. در مجموع ۲۸۳۵۴۵۲۲۳۳۴۶ مسیر در تست جعبه سیاه و سفید گنجانده شدند و نتایج به پوشش ۹۹/۸۷٪ مسیر ترجمه شد. یکی از ایرادات نرم‌افزار در طول تست جعبه سیاه و سفید شناسایی شد. تست جعبه سفید مستلزم تست POCKET با دانش عملکرد داخلی نرم‌افزار صورت می‌گیرد و برای مسیرهای دشوار تست مورد استفاده قرار می‌گیرد مانند مسیرهایی که توسط برخی ورودی‌های تابع، محدود یا غیرقابل آزمایش گردیده‌اند. ۳۷۳۲۹۳۱۴۶ مسیر باقی‌مانده را تجزیه و تحلیل نمودیم و ۱۰ مسیر را غیرقابل آزمایش تشخیص دادیم، چرا که آن‌ها نتیجه دو جمله شرطی بودند. شرط یک جمله 'if'، شرط 'else' جمله 'if' دیگر بود که هرچند از لحاظ نظری امکان‌پذیر است ولی در عمل قرار گرفتن آن‌ها در یک مسیر غیرممکن است. مشخص شد که هفته مسیر به دلیل سبک کد نویسی حشو هستند. آن‌ها در کد نویسی اصلاح گردیدند.

جدول ۳- اصول طراحی

محیط	اصول طراحی
حقوقی	POCKET باید راهی برای شناسایی روش‌های حریم خصوصی سایت فراهم کند. POCKET باید فرآیند رضایت والدین برای آشکارسازی و استفاده از اطلاعات فرزندشان را به صورت مرحله‌به‌مرحله طبق ترجیحات از پیش تعیین‌شده والدین، خودکار نماید. POCKET باید روشی برای پدر و مادر فراهم کند تا اطلاعاتی که توسط سایت فراهم‌شده را مرور کنند و اگر نیاز به حذف اطلاعات باشد وبسایت را مطلع سازند. POCKET باید از اطلاعاتش محافظت کرده و اطلاعات صحیحی به تاجران وبسایت که اطلاعات را از طرف والدین با آن‌ها به اشتراک می‌گذارد، ارائه دهد.
فنی	POCKET باید به‌سادگی قابل دانلود باشد. نصب POCKET باید ساده باشد. رابط کاربر باید گرافیکی بوده و با استفاده از آیتم‌های منو و جعبه‌های دیالوگ کاربر را به راحتی هدایت کند؛ فهم پیام‌های خطا نیز باید ساده باشد. POCKET باید در ابتدا با استفاده از شیء کمک‌کننده به مرورگر (BHO) برای اینترنت اکسپلورر توسعه یابد.

مرحله انتقال (چه انتقال اطلاعات تأیید شده باشد چه نه) باید هنگام نصب و کار با POCKET شفاف باشد. POCKET به انتقال مطمئن اطلاعات بین والدین، وبسایت و ماشین‌های شخص ثالث نیاز دارد. POCKET باید با استفاده از مفهوم عامل کاربری P3P به صورت خودکار فایل ترجیحات حریم خصوصی خود را با فایل روش‌های حریم خصوصی مقایسه کند. POCKET باید والدین را قادر سازد تا تنظیمات را به دلخواه تغییر دهد. POCKET باید شامل ۴ فاز باشد: ثبت نام، نصب، تراکنش و فاز پس تراکنش	
POCKET باید برای استفاده آسان باشد. POCKET باید نیازمندی‌های حقوقی را تأمین نماید. POCKET باید برای استفاده والدین فایل‌های ثبت وقایع ایجاد کنند. POCKET باید بر روی اطلاعاتی که توسط فرزندان آشکار می‌گردد کنترل بیشتری فراهم کند. POCKET باید بیش‌ترین بهره‌وری را با کم‌ترین هزینه فراهم کند.	رفتاری

جدول ۴- ارزیابی حقوقی POCKET

شواهد ارزیابی	اصول طراحی
POCKET فایل ترجیحات حریم خصوصی را با سیاست‌های امنیتی وبسایت مقایسه می‌کند.	POCKET باید راهی برای شناسایی روش‌های حریم خصوصی سایت فراهم کند.
طی فاز راه‌اندازی، والدین اطلاعاتی که می‌تواند آشکار گردد را مشخص می‌کنند. انتخاب‌های والدین باید با وبسایت‌هایی که اطلاعات کودکان را جمع‌آوری می‌کنند تطابق یابد تا اطلاعات به صورت موفقیت‌آمیزی با وبسایت مذکور به اشتراک گذاشته شود.	POCKET باید فرآیند رضایت والدین برای آشکارسازی و استفاده از اطلاعات فرزندان را به صورت مرحله‌به‌مرحله طبق ترجیحات از پیش تعیین شده والدین، خودکار نماید.
POCKET یک فایل ثبت وقایع ایجاد می‌کند. سپس، یک قرارداد دیجیتالی ایجاد شده و همراه با اطلاعات شخصی برای سایت ارسال می‌شود. فایل ثبت وقایع و قرارداد دیجیتالی می‌توانند برای جواب‌گویی تاجر به درخواست‌های والدین مورد استفاده قرار گیرند.	POCKET باید روشی برای پدر و مادر فراهم کند تا اطلاعاتی که توسط سایت فراهم شده را مرور کنند و اگر نیاز به حذف اطلاعات باشد وبسایت را مطلع سازند.
POCKET با معیارهایی طراحی شده که انتقال و ذخیره‌سازی ایمن اطلاعات را ممکن می‌سازد. در ادامه، برای اطمینان از صحت و درستی، POCKET با استفاده از P3P گسترش یافته ایجاد شده بود، که شامل تگ گذاری صحیح برای اطلاعات ارسالی به وبسایت‌های تاجران می‌باشد.	POCKET باید از اطلاعاتش محافظت کرده و اطلاعات صحیحی به تاجران وبسایت که اطلاعات را از طرف والدین با آن‌ها به اشتراک می‌گذارد، ارائه دهد.

به‌طور خلاصه، از آنجایی که ۱۰۰٪ پوشش دستورات و ۱۰۰٪ پوشش مسیر، به‌اندازه کافی بسنده تشخیص داده شدند تا بتوانیم بگوییم سیستم مورد آزمایش قرار گرفت، POCKET به‌طور گسترده و به‌اندازه کافی تست‌شده است. مرحله دوم ارزیابی فنی آزمون، تأیید رعایت اصول فنی طراحی بود. جدول ۵ نشان می‌دهد که هر یک از اصول طراحی پیشنهادی و نتایج موردبررسی قرار گرفتند. به‌طور خلاصه، POCKET از نمونه‌ای از ابزارها و مفاهیم موجود نظریه‌های هسته‌ای ارائه‌شده در بخش ۴-۳، بهره می‌گیرد و شرایط از پیش تعیین‌شده را رعایت می‌کند. بسیاری از اصول طراحی مشتق شده از این نظریه‌های هسته و محیط فنی نیز در ارزیابی رفتاری (کاربر) مانند سهولت کاربرد و ناوبری مورد آزمایش قرار گرفتند.

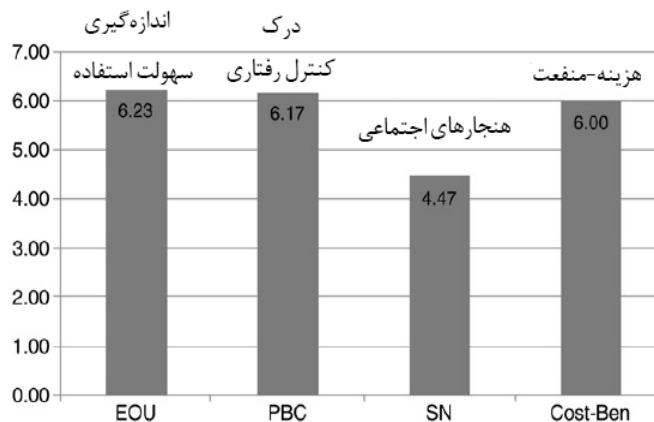
جدول ۵- ارزیابی حقوقی POCKET

شواهد ارزیابی	اصول طراحی
تست جعبه سیاه	POCKET باید به‌سادگی قابل دانلود باشد.
تست جعبه سیاه	نصب POCKET باید ساده باشد.
-----	رابط کاربر باید گرافیکی بوده و با استفاده از آیتم‌های منو و جعبه‌های دیالوگ کاربر را به راحتی هدایت کند؛ فهم پیام‌های خطا نیز باید ساده باشد.
تست جعبه سیاه	POCKET باید در ابتدا با استفاده از شیء کمک‌کننده به مرورگر (BHO) برای اینترنت اکسپلورر توسعه یابد.
تست جعبه سیاه	مرحله انتقال (چه انتقال اطلاعات تأییدشده باشد چه نه) باید هنگام نصب و کار با POCKET شفاف باشد.
تست جعبه سیاه	POCKET به انتقال مطمئن اطلاعات بین والدین، وب‌سایت و ماشین‌های شخص ثالث نیاز دارد.
تست جعبه سیاه	POCKET باید با استفاده از مفهوم عامل کاربری P3P به صورت خودکار فایل ترجیحات حریم خصوصی خود را با فایل روش‌های حریم خصوصی مقایسه کند.
تست جعبه سیاه	POCKET باید والدین را قادر سازد تا تنظیمات را به‌دلخواه تغییر دهند.
تست جعبه سیاه	POCKET باید شامل ۴ فاز باشد: ثبت‌نام، نصب، تراکنش و فاز پس تراکنش

ارزیابی کاربر/ طراحی:

همان‌طور که شکل ۱، نشان می‌دهد، نتایج ارزیابی تمام معیارهایی که می‌توان از طریق توسعه POCKET کنترل نمود (سهولت استفاده، کنترل رفتاری، و هزینه - منفعت) نشان می‌دهد که پدر و مادرها بر این عقیده‌اند که POCKET انتظارات آن‌ها را برآورده می‌کند، که نشان می‌دهد ما در ایجاد

ابزاری که پاسخ‌گوی نیازهای بیان شده والدین قبل از طراحی POCKET باشد، موفق بوده‌ایم. ساختار هنجار اجتماعی، که نمی‌تواند در توسعه POCKET کنترل شود، نیز بالاتر از نقطه میانی مقیاس، بوده است که نشان می‌دهد هرچند این عامل مهم‌ترین عامل در تعیین ظرفیت استفاده پدر و مادر از POCKET نیست، ولی آنچه دیگر والدین انجام می‌دهند، برای تعیین استفاده والدین از POCKET مهم می‌باشد. همان‌طور که از جدول ۶ مشاهده می‌شود، POCKET با موفقیت شرایط و الزامات طراحی رفتاری را برآورده می‌کند. اعتبار طراحی POCKET پیش‌تر از سوی وب، از طریق مصاحبه با دو تن از صاحبان وبسایت، مورد تأیید قرار گرفت. یکی از آن‌ها صاحب یک وبسایت خرده‌فروشی بر خط است و دیگری صاحب یک وبسایت خدمات ورزشی است. هیچ‌کدام از این دو مالک وبسایت از الزامات قانونی، آگاه نبودند، اگرچه هر دو مالک می‌توانستند از آن الزامات پیروی کنند. هر دو مالک ابراز نمودند که مفهوم POCKET و محصول حاصل از آن را می‌پسندند. و اگر از انطباق POCKET با قانون اطمینان حاصل کنند، از آن استفاده خواهند کرد. با این حال، آن‌ها نیز ابراز نمودند که از نرم‌افزار POCKET استفاده نخواهند کرد مگر آن که جمعیت کثیری از والدین نیز از آن استفاده کنند. این موضوع باعث ایجاد مسئله معرف مرغ و تخم مرغ می‌شود، زیرا پدر و مادرها نیز می‌گویند که آن‌ها زمانی از POCKET استفاده خواهند که دیگر والدین نیز از آن استفاده کنند.



شکل ۱: مقایسه میانگین معیارهای ارزیابی رفتاری

جدول ۶- ارزیابی حقوقی POCKET

اصول طراحی	شواهد ارزیابی
POCKET باید برای استفاده آسان باشد.	همان‌طور که در شکل ۱ نشان داده شد، نظرخواهی از والدین نشان داد که آن‌ها معتقدند که POCKET برای استفاده آسان است.
POCKET باید نیازمندی‌های حقوقی را تأمین نماید.	همان‌طور که در ارزیابی حقوقی نشان داده شد، POCKET شرایط لازم حقوقی را برطرف می‌نماید.
POCKET باید برای استفاده والدین فایل‌های ثبت وقایع ایجاد کند.	همان‌طور که در ارزیابی حقوقی نشان داده شد، POCKET فایل‌های ثبت وقایع ایجاد می‌کند. به علاوه، طراحی POCKET شامل حالت والدین و حالت کودک است. یکی از مزایای حالت والدین این است که حفاظت POCKET و توانایی لاگ برداری خاموش می‌شود.
POCKET باید بر روی اطلاعاتی که توسط فرزندان آشکار می‌گردد کنترل بیشتری فراهم کند.	همان‌طور که در شکل ۱ نشان داده شد، نظرخواهی از والدین در رابطه با POCKET نشان می‌دهد که آن‌ها معتقدند این نرم‌افزار کنترل آن‌ها را افزایش می‌دهد.
POCKET باید بیش‌ترین بهره‌وری را با کم‌ترین هزینه فراهم کند.	POCKET برای والدین قابل دانلود است، به علاوه همان‌طور که در شکل ۱ نشان داده شد، POCKET در ارزیابی والدین از لحاظ هزینه - منفعت رتبه بالایی داشت.

۵- بحث

POCKET یک نمونه اولیه است و برای برآورده نمودن الزامات قانونی طراحی شده است و برای والدین ابزاری برای محافظت از حریم خصوصی بر خط کودکان فراهم می‌کند. در طراحی POCKET، ما از اصول علم طراحی ارائه شده توسط Hevner و همکارانش در سال ۲۰۰۴، بهره گرفتیم، آن‌ها بر این باورند که پژوهش‌ها در زمینه سیستم‌های اطلاعاتی تحت تأثیر «مردم، سازمان‌ها، و تکنولوژی» قرار دارند. تحقیقات طراحی بخش مهمی از حوزه سیستم‌های اطلاعاتی است. Orlikowski و Iacono در سال ۲۰۱۴، پنج طبقه را توصیف می‌کنند که پژوهش‌های طراحی را ترسیم می‌کند، دیدگاه ابزاری، دیدگاه نماینده، دیدگاه گروه، دیدگاه محاسباتی، و دیدگاه اسمی. دیدگاه ابزاری بر توصیف "ویژگی‌های فنی یک فناوری جدید تمرکز دارد تا بدانیم که آن فناوری چه چیزی انجام خواهد داد.

Orlikowski و Iacono در سال ۲۰۱۴، استدلال می‌کنند که این رویکرد، پژوهش سیستم‌های اطلاعاتی را به چیزی بیش از رویکرد جعبه سیاه محدود می‌کند و نشان می‌دهند که محققان سیستم‌های اطلاعاتی باید در جهت ارائه مفهومی قوی‌تر از نحوه کاربرد فناوری اطلاعات در درون سازمان‌ها تلاش

کنند. جالب است که یکی از مسائل مشترک دانشمندان علوم اجتماعی این است که آن‌ها محصولات را اغلب به شکل جعبه‌های سیاه ارائه می‌کنند. دیدگاه نماینده بر "یک یا تعداد کمی از عناصر کلیدی مشترک تمرکز می‌کند، که نشان‌دهنده و یا نماینده جنبه ضروری، ویژگی، یا ارزش فناوری اطلاعات هستند. "دیدگاه محاسباتی" به صراحت بر قدرت محاسباتی فناوری اطلاعات تمرکز می‌کند. "این نوع پژوهش طراحی، بر قابلیت‌های فناوری برای نشان دادن، دست‌کاری، ذخیره، بازیابی، و انتقال اطلاعات، و در نتیجه پشتیبانی، پردازش، مدل‌سازی، یا شبیه‌سازی جنبه‌های جهان تمرکز دارد." دیدگاه اسمی فناوری، فناوری را غایب قلمداد می‌کند، و نشان می‌دهد که "فناوری فقط در نام تجلی می‌یابد نه در واقعیت." درنهایت، دیدگاه جمعی فناوری مستلزم آن است که محققان توضیح دهند که چگونه اجزای یک محصول طراحی شده را می‌توان به یک فعالیت اجتماعی و اقتصادی اعمال نمود. این دیدگاه بر تعامل فناوری مورد استفاده، افراد درگیر در فرآیند طراحی، و همچنین مخاطبان هدف محصول نهایی تمرکز می‌کند. در این تحقیق، ما چالش Orlowski و Iacono را پذیرفتیم و در این راستا توضیح دادیم که چگونگی طراحی POCKET متأثر از سه رشته و اثر متقابل آن‌ها بوده است و نشان دادیم که چگونه POCKET توسط تیم طراحی و همچنین مخاطبان هدف مورد آزمایش قرار گرفت. این به‌وضوح نمایانگر دیدگاه جمعی است. جالب است که Orlowski و Iacono در بررسی مقالات مجلات پژوهشی سیستم‌های اطلاعاتی دریافتند که دیدگاه جمعی دارای کوچک‌ترین طبقه‌بندی (کم‌ترین نمایندگی) بوده است. توصیه آن‌ها به استفاده از دیدگاه جمعی، "که با جنبه‌های اجتماعی و تعبیه‌شده توسعه فناوری و کاربرد آن" درگیر نمی‌شود، شامل کسب اطمینان از بررسی شرایط مادی و فرهنگی است که محصولات فناوری اطلاعات را به یکدیگر پیوند می‌دهد و ماهیت پویای آن‌ها را بررسی می‌کند. در توسعه POCKET از این توصیه‌ها پیروی شده است و به حجم پژوهش‌های صورت گرفته که به صراحت به موضوع محصولات فناوری اطلاعات پرداخته‌اند، می‌افزاید. تحقیق حاضر علاوه بر پاسخ دادن به تقاضاها برای تحقیقات بیشتری که به صراحت به موضوع محصولات IT در بافت اجتماعی- فنی خود پرداخته‌اند، نشان می‌دهد که چگونه دستورالعمل پیشنهادشده توسط Hevner در سال ۲۰۰۴، به محققان علم طراحی اجازه می‌دهد تا در جعبه سیاه را از آثار خود بردارند. نحوه پیروی از این هفت دستورالعمل در جدول ۷ آمده است. به‌طور خلاصه، فایده این مطالعه به جنبه مباحث طراحی و نظری که توسط Gregor در سال ۲۰۰۶، ارائه شده است، مربوط می‌شود. محصولی بر اساس دستورالعمل‌های علمی تعیین شده، طراحی گردید. در نتیجه، به‌طور کلی نتایج این پژوهش نسبت به کارهای قبلی در زمینه حفظ حریم خصوصی اطلاعات، ابزارهای

افزایش حریم خصوصی و پژوهش علم طراحی از رشد تصاعدی برخوردار بوده است. علاوه بر این، همان‌طوری که Bélanger در سال ۲۰۱۲، ابراز می‌دارد از منظر پژوهشی، این مطالعه نشان‌دهنده ارزش رویکرد پژوهشی گروه متمرکز است.

جدول ۷- دستورالعمل‌های علم طراحی و POCKET

نویسنده	دستورالعمل‌های طراحی	انطباق POCKET
Livingstone S, Helsper E J (۲۰۰۸).	مشکل ارتباط	POCKET نیاز به فناوری برای اجرای قوانین محافظت از حریم خصوصی بر خط کودکان را برآورده می‌سازد؛ قوانین محافظت از حریم خصوصی بر خط کودکان قوانینی هستند که در خصوص محافظت از حریم خصوصی بر خط کودکان می‌باشد.
Cranor L.F. (۲۰۰۳).	طراحی به عنوان یک فرآیند پژوهشی	طراحی قوانین محافظت از حریم خصوصی بر خط کودکان از طراحی و فرآیندهای آزمون دقیق پیروی می‌کند. در توسعه POCKET، قانون به‌طور گسترده بررسی می‌گردد تا اطمینان حاصل شود که POCKET الزامات قانونی قوانین محافظت از حریم خصوصی بر خط کودکان را برآورده نموده است. گروه‌های متمرکز تشکیل داده شدند تا اطمینان حاصل شود که بهترین روش‌ها در POCKET تعبیه شده است. آزمون شامل آزمون جعبه سیاه و جعبه سفید بود.
Schneider J P, Corley M D, Irons R R (۱۹۹۸).	طراحی به عنوان یک محصول	نتیجه این تحقیق، برنامه POCKET است.
Bélanger F. (۲۰۱۲).	ارزیابی طراحی	ارزیابی POCKET شامل ارزیابی‌های حقوقی، فنی، و رفتاری بود.
Bélanger F, Crossler R.E (۲۰۱۱).	دقت تحقیق	توسعه POCKET به تبعیت از روش‌های طراحی صورت گرفته در پژوهش‌های علم طراحی، ثابت شده‌اند. به همین ترتیب بررسی POCKET شامل یک فرآیند ارزیابی دقیق بود.
Casilli, A. A. Tubaro, P. & Araya, P (۲۰۱۲).	نتایج و فواید تحقیق	POCKET پیاده‌سازی محصولی است که حاصل توسعه P3P است که مکانیسم‌هایی برای پاسخ‌گویی و اجرای قوانین محافظت از حریم خصوصی بر خط کودکان فراهم می‌کند.
Cranor L.F. Byers S, Kormann D (۲۰۰۳)	ارتباطات تحقیق	در این مقاله، ما این محصول را با بخش‌هایی ارائه کردیم که برای مخاطبان با رویکردی مدیریتی در نظر گرفته شده و همچنین بخش‌هایی برای بیان طرح به مخاطبان فنی مدنظر گرفته شده است.

پیشنهادهای:

توسعه و آزمایش محصول POCKET اولین گام کوچک در جهت حفاظت از حریم خصوصی بر خط کودکان است. در این بخش، ما به‌طور خلاصه برخی از ایده‌های دیگر را برای تحقیقات آینده مورد بحث قرار می‌دهیم. در ابتدا، از آنجایی که پژوهش‌هایی که با استفاده از روش POCKET شروع شده‌اند ادامه دارند، این پژوهش‌ها باید به سمت حفاظت از حریم خصوصی کودکان در یک محیط محاسباتی تلفن همراه سوق داده شود. برنامه‌های موبایلی که برای استفاده کودکان طراحی شده‌اند، در خط‌مشی حریم خصوصی خود به‌وضوح بیان نمی‌کنند که این برنامه‌ها چگونه به جمع‌آوری داده می‌پردازند و یا چگونه با سایت شبکه‌های اجتماعی تعامل دارند. با این حال، مقررات قانونی در تلاش برای تهیه تبصره‌هایی در مواردی است تا صریحاً برنامه‌های تلفن همراه را نیز در خود بگنجانند، هم‌چنین تعریف "اطلاعات شخصی" را گسترش دهد و چیزهایی مانند شناسان گر دستگاه، اطلاعات جغرافیایی محل، و آدرس IP را در خود بگنجانند. اعمال چنین تغییراتی در قوانین نشان‌دهنده این است که در محیط محاسباتی تلفن همراه همانند محیط رایانه‌های شخصی، نیاز فزاینده‌ای به طراحی نرم‌افزارهایی مانند POCKET وجود دارد. از آنجایی که نسخه‌های آتی POCKET ساخته می‌شوند، توجه‌ها باید به گسترش پوشش POCKET برای افزودن دیگر اطلاعات شخصی قابل‌شناسایی مانند موقعیت مکانی، اطلاعات شخصی در کوکی‌های تلفن همراه، و دستگاه‌های شناسان گر متمرکز شود. با اعطای این توانایی به پدر و مادرها برای کنترل دقیق اطلاعاتی که کودکانشان در حین استفاده از تلفن همراه می‌توانند به مشارکت بگذارند، کنترل به والدین باز می‌گردد. در صورت عدم وجود فرمی از اجرای فناوری، تضمینی وجود ندارد که برنامه‌های تلفن همراه در حال جمع‌آوری این اطلاعات نباشند. POCKET علاوه بر برآوردن الزامات فنی و رفتاری مشخص شده، به‌طور خاص برای برآوردن الزامات قانونی، ایجاد می‌گردد. البته چارچوب‌های حقوقی دیگری در مورد اطلاعات مالی و سلامت بر خط وجود دارد. هم‌چنین برای کشورهای مختلف در سراسر جهان چارچوب‌های حقوقی مختلفی وجود دارد. بنابراین، یکی از راه‌های بالقوه برای تحقیقات آینده انطباق POCKET با این چارچوب‌های قانونی متفاوت است.

محدودیت‌ها:

یکی از محدودیت‌های این تحقیق، همانند اکثر پژوهش‌های علم طراحی، این است که نمی‌توان استفاده مستمر را ارزیابی نمود. استفاده مستمر در مقایسه با قصد استفاده، می‌تواند شاخص مهم‌تری برای

ارزیابی محصولات باشد. این موضوع با استدلال رفتارهای انتخابی همخوانی دارد و در آن تأکید می‌شود که اگرچه سازمان‌ها در طیف گسترده‌ای از سیستم‌های اطلاعاتی سرمایه‌گذاری نمودند، کاربران بالقوه بسیاری از این نرم‌افزارها، خیلی کم از آن‌ها استفاده می‌کنند. با این حال، این امر نیازمند این است که جمعیت کثیری از والدین و مدیران وب تصمیم به استفاده از POCKET بگیرند و این‌که این نرم‌افزار توسط سازندگان مرورگرها در مرورگرهایی نظیر اینترنت اکسپلورر گنجانیده شود. از آنجایی که بسیاری از مدیران وب ترجیح می‌دهند جمع‌آوری داده خود را محدود نکنند، این احتمال وجود دارد که این حالت فقط در صورت کاربرد اجباری یک سازمان دولتی محقق گردد.

۶- نتیجه‌گیری

در این مقاله، ما محصول جدیدی به نام POCKET را برای تقویت حریم خصوصی و اخلاقی معرفی نمودیم که به عنوان یک نمونه اولیه برای حفاظت از حریم خصوصی بر خط کودکان طراحی شده است. POCKET روشی خودکار برای به دست آوردن رضایت والدین اجرا می‌کند که در قوانین محافظت از حریم خصوصی بر خط کودکان ذکر شده است. این برنامه به آسانی قابل استفاده است و والدینی که از دانش بالای رایانه برخوردار نیستند نیز می‌توانند از آن برای محافظت از حریم خصوصی فرزندان خود بهره بگیرند. والدین با استفاده از POCKET، می‌توانند بدون آن‌که همیشه بر فعالیت‌های بر خط کودکانشان نظارت داشته باشند، اطلاعات شخصی که توسط وبسایت‌ها از کودکان جمع‌آوری می‌شود را کنترل کنند. ترجیحات کاربر و سیاست‌های تجاری، قالبی دارند که با مشخصات P3P سازگار است. برنامه POCKET فرض را بر این می‌گیرد که سیاست‌های تجاری در یک محل خاص بر روی سرور قرار داده شده است و POCKET شامل یک پروتکل امن برای آپلود اطلاعات شخصی از سوی مشتری به تاجر می‌باشد. همچنین این برنامه مکانیسمی برای پاسخ‌گویی مدیران فراهم می‌کند. با وجود وبسایت‌های تجاری ساختگی، نمونه اولیه برنامه، توانایی خود را در ارائه یک پلتفرم سازگار با قوانین محافظت از حریم خصوصی بر خط کودکان نشان داده است. ارزیابی‌های انجام‌شده نشان می‌دهد که این ابزار فاقد باگ نرم‌افزاری است و نیازهای والدین در حفاظت از حریم خصوصی بر خط فرزندان را برآورده می‌کند.

این پژوهش هم برای محققان و هم عموم مردم به‌طور یکسان فایده بخش است. از دیدگاه پژوهشی، POCKET نشان می‌دهد که چگونه فناوری‌های موجود مانند P3P می‌توانند برای ارائه راه‌حل عملی برای تبادل اطلاعات درباره اشخاص ثالث مورد استفاده قرار گیرند. همچنین این برنامه نشان می‌دهد

که چگونه می‌توان به گروه‌های متمرکز برای اطلاع‌رسانی در مورد توسعه یک نرم‌افزار اتکا نمود. POCKET منجر به نتایج مهمی در پژوهش‌های طراحی می‌شود چرا که به پایه دانش در مهندسی کامپیوتر، سیستم‌های اطلاعاتی و قانون کسب‌وکار می‌افزاید. محققان آینده می‌توانند با بیان کشفیات صورت گرفته در طول توسعه POCKET، در مورد تحقیقات خود اطلاع‌رسانی کنند و همچنین در مورد آنچه در این پروژه انجام شد، شرح مبسوطی ارائه دهند.

این پژوهش ابزار واقعی فراهم می‌کند که هرگاه به‌طور کامل اجرا شود، می‌تواند لایه مضاعفی برای حفاظت از والدین فراهم کند تا آن‌ها در حفاظت از حریم خصوصی بر خط کودکانشان بر آن تکیه کنند. استفاده از گروه‌های متمرکز همراه با ارزیابی محصول نهایی نشان می‌دهد که این ابزار الزاماتی را که والدین ابراز نمودند، برآورده می‌کند.

ملاحظه‌های اخلاقی

واژه کودکان در این مقاله، به افراد زیر سن ۱۳ سال اشاره دارد. پردازش داده‌های شخصی کودکان قانونی و اخلاقی بوده که در ابتدا، توسط والدین کودکان اجازه داده شده است (در مقررات محافظت از اطلاعات عمومی، پردازش داده‌های شخصی کودکان باید قانونی باشد و زمانی مجاز شمرده می‌شود که توسط والدین کودک اجازه داده شود).

سپاس‌گزاری:

در پایان از تمامی مدیران و کارکنان شرکتی که نمونه‌گیری در آن انجام گرفته و امکان اجرای این تحقیق را فراهم ساختند تشکر و قدردانی می‌نماییم و از سرکار خانم دکتر محبوبه مشکین فام که به غنای مطالب این تحقیق افزودند کمال تشکر را داریم.

کتابنامه

- Bélanger F. (2012). Information systems theorizing using focus groups, *Australasian Journal of Information Systems* 17 (2): 109–135.
- Bélanger F, Crossler R.E. (2011). Privacy in the digital age: a review of information privacy research in information systems, *MIS Quarterly* 35 (4): 1017–1041.
- Boyd D. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media*. Cambridge, MA: MIT Press. pp. 119–142.
- Casilli, A. A. Tubaro, P. & Araya, P. (2012). Ten years of Ana: Lessons from a transdisciplinary body of literature on online proeating disorder websites. *Social Science Information*, 51(1): 120–139.
- Cranor L.F. (2003). P3P: making privacy policies more useful, *IEEE Security & Privacy Magazine* 1 (6) 50–55.
- Cranor L.F. Byers S, Kormann D. (2003). An analysis of P3P deployment on commercial, government, and children's web sites as of may 2003, in: Technical report, AT&T Labs-Research.
- Gregor S. (2006). The nature of theory in information systems, *MIS Quarterly* 30 (3): 611–642.
- Hevner A R, March ST, Park J, Ram S. (2004). Design science in information systems research, *MIS Quarterly* 28 (1):75–105.
- Livingstone S, Bober M. (2005). UK children go online: Final report of key project findings. London School of Economics and Political Science. Accessed 15 February 2013. The Internet, children, and privacy 273.
- Livingstone S, Bober M. (2006). Regulating the Internet at home: Contrasting the perspectives of children and parents. In D. Buckingham & R. Willett (Eds.), *Digital generations: Children, young people, and new media* Mahwah, NJ: Lawrence Erlbaum Associates, Publishers. (pp. 93–113.
- Livingstone S, Helsper E J. (2008). Parental mediation of children's Internet use. *Journal of Broadcasting and Electronic Media*, 52(4): 581–599.

- Marwick A E. (2008). To catch a predator? The Myspace moral panic. First Monday, 13(6). <http://firstmonday.org/ojs/index.php/fm/article/view/2152/1966>. Accessed 22 July 2013.
- Marwick A E, Diaz MD, Palfrey J. (2008). Youth, privacy and reputation. Berkman Center for Internet and Society. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163. Accessed 5 November 2012. 2010.
- Mont MC, Bramhall P. (2014). Ibe applied to privacy and identity management trusted, in: Technical Report, HP Laboratories, Bristol.
- Muntermann J. (2015). Towards ubiquitous information supply for individual investors: a decision support system design, Decision Support Systems 47 (2): 82–92.
- Ngai EWT, Leung TKP, Wong YH, Lee MCM, Chai PYF, Choi YS. (2012). Design and development of a context-aware decision support system for real-time accident handling in logistics, Decision Support Systems 52 (4): 816–827.
- Orlikowski WJ, Iacono CS. (2014). Research commentary: desperately seeking “IT” in IT research—a call to theorizing the IT artifact, Information Systems Research 12 (2): 121–134.
- Ratnasingam P. (2015). The importance of technology trust in web services security, Information Management & Computer Security 10 (5): 255–260.
- Schneider J P, Corley M D, Irons R R. (1998). Surviving disclosure of infidelity: Results of an international survey of 164 recovering sex addicts and partners. Sexual Addiction & Compulsivity, 5 (3): 189–218.
- Taylor S, Todd PA. (2014). Understanding information technology usage: a test of competing models, Information Systems Research 6 (2): 144–176.
- Venkatesh V, Morris M, Davis G, Davis F. (2014). User acceptance of information technology: toward a unified view, MIS Quarterly 27 (3): 425–478.

