Engaging Children About Online Privacy Through Storytelling in an Interactive Comic

Leah Zhang-Kennedy
Carleton University
Ottawa, Canada
leah.zhang@carleton.ca

Khadija Baig
Carleton University
Ottawa, Canada
khadijabaig@cmail.carleton.ca

Sonia Chiasson
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

Children's privacy is put at risk through online sharing of location-based information. We study the effectiveness of an educational interactive comic on improving 11- to 13-year-old children's privacy knowledge and behaviour immediately and one week after reading. Children's privacy knowledge increased after reading either the comic or the text-only control, but the comic promoted superior knowledge retention a week later and was more successful at influencing children's reported privacy behaviour than the control. Our 22 child-parent pairs found the comic facilitated learning for children, engaging, and easy to use. We discuss the implication on children's short and long-term knowledge retention and behaviour, and the educational potential of comics at addressing the challenges of privacy and security education for children.

Privacy; Comics; Children; Education; Human-Computer Interaction; Mobile

1. INTRODUCTION

Turner and Harviainen (2016) describe pretending/make-believe as a form of cognition complementary to problem solving that enables users to create and access other environments. Pretending is essential to child development as a form of play (Leslie 1987), and involves generating ideas and creating emotions (Turner and Harviainen 2016). Role-playing through stories enables children to acquire and practice communication, problem solving, and empathy (Hughes 2009).

We explore storytelling and make-believe through Secure Comics, an interactive comic that we designed to get children thinking about online privacy. As more children go online using portable devices from a variety of physical locations (Steeves 2012), there is an increasing need to educate them on ways to protect their online privacy. Smartphones equipped with GPS are capable of tracking and transmitting users' location, putting them at risk of behavioural advertising, identity theft, and stalking (Friedland and Sommer 2010). Users often reveal sensitive information without their explicit knowledge in a process called geo-tagging that automatically attaches metadata containing personal information to photos taken with smartphones (Friedland and Sommer 2010).

Although privacy enhancing software and parental supervision reduce children's privacy risks, they do not empower children to make informed decisions online, or help them develop practical skills for managing their online privacy. Children's privacy researchers recommend that privacy and security educational tools should teach children to critically think about the consequences of their online actions (Steeves 2012), improve their mental models (Zhang-Kennedy et al. 2016), and influence their behaviour (Sharples et al. 2009).

Walton (1990) suggests that engaging fictions encourage the audience to engage in make-believe. Our study provides some evidence on the role of digital visual narratives like comics at influencing children's knowledge and behaviour. Using a between-subject study design (*Comic* vs. same-narrative *Text*) with 22 child-parent pairs, we found that both narrative types showed statically significant improvements in privacy knowledge immediately after reading, but the *Comic* was more effective for retaining knowledge after one week. Furthermore, the comic was persuasive in changing children's reported privacy behaviour. Participants found the comic engaging, easy to use, and easy to learn. We discuss the implication on children's short and long-term knowledge retention and behaviour, and the educational potential of comics at addressing the challenges of privacy and security education.

Authors' copy (version: May 9, 2017). To appear in British HCI 2017.

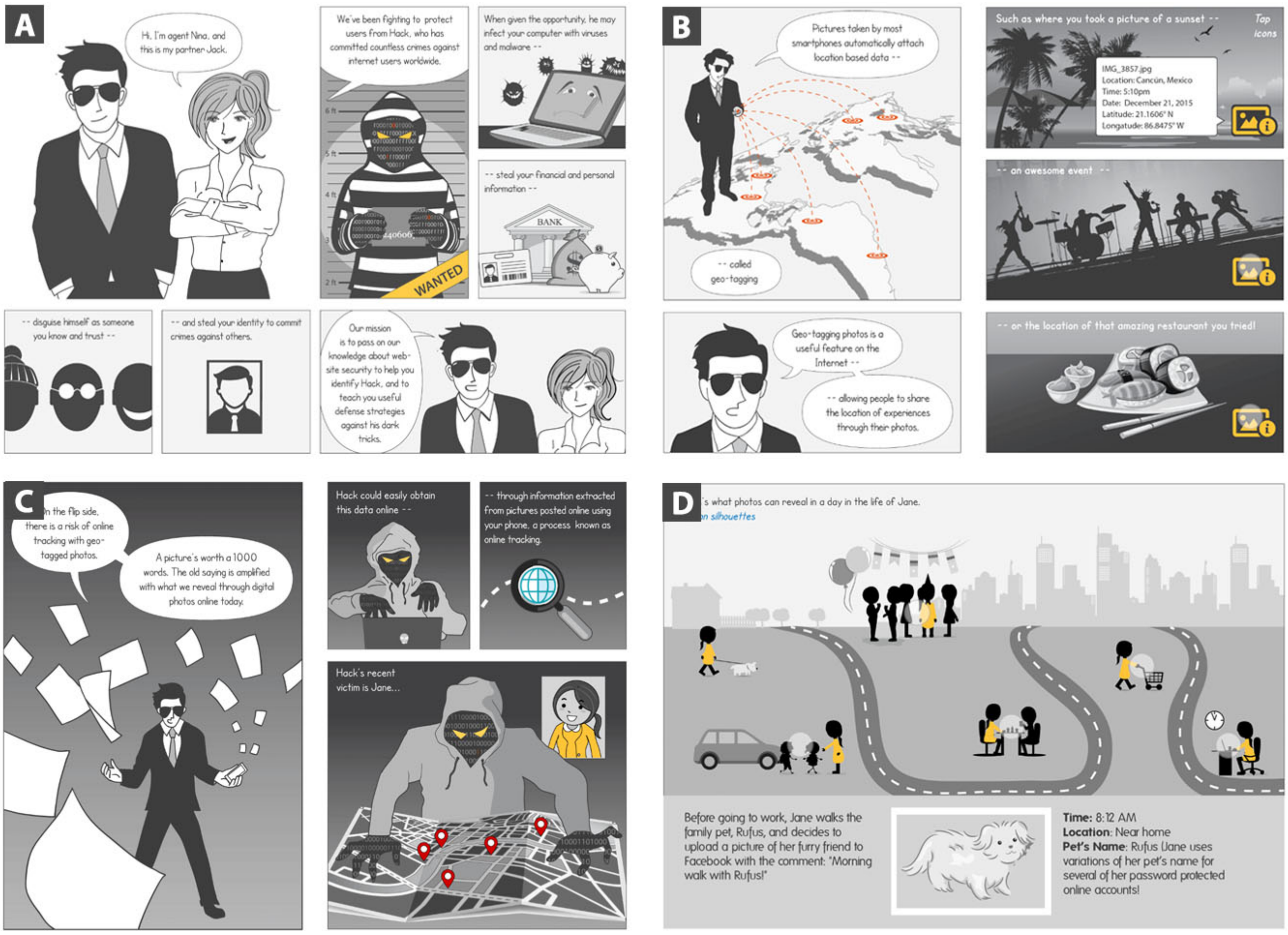

A
Hi, I'm agent Nina, and this is my partner Jack.
We've been fighting to protect users from Hack, who has committed countless crimes against internet users worldwide.
6 ft
5 ft
4 ft
3
2 ft
240606
WANTED
When given the opportunity, he may infect your computer with viruses and malware --
-- steal your financial and personal information --
BANK
-- disguise himself as someone you know and trust --
-- and steal your identity to commit crimes against others.
Our mission is to pass on our knowledge about web-site security to help you identify Hack, and to teach you useful defense strategies against his dark tricks.
B
Pictures taken by most smartphones automatically attach location based data --
-- called geo-tagging
Such as where you took a picture of a sunset --
Tap icons
IMG_3857.jpg
Location: Cancún, Mexico
Time: 5:10pm
Date: December 21, 2015
Latitude: 21.1606° N
Longatude: 86.8475° W
-- an awesome event --
Geo-tagging photos is a useful feature on the Internet --
-- allowing people to share the location of experiences through their photos.
-- or the location of that amazing restaurant you tried!
C
n the flip side, there is a risk of online tracking with geo-tagged photos.
A picture's worth a 1000 words. The old saying is amplified with what we reveal through digital photos online today.
Hack could easily obtain this data online --
-- through information extracted from pictures posted online using your phone, a process known as online tracking.
Hack's recent victim is Jane...
D
's what photos can reveal in a day in the life of Jane.
n silhouettes
Before going to work, Jane walks the family pet, Rufus, and decides to upload a picture of her furry friend to Facebook with the comment: "Morning walk with Rufus!"
Time: 8:12 AM
Location: Near home
Pet's Name: Rufus (Jane uses variations of her pet's name for several of her password protected online accounts!

Figure 1: *Sample screens from Secure Comics's privacy chapter. Screens B & D have interactive features. A) Intro; B) Geotagging (with interactive picture icons); C) Online tracking; D) A day in the life of Jane (with interactive activities map). Note: navigation is cropped to save space.*

2. BACKGROUND

Comics use linguistic, visual, gestural, and spatial conventions to communicate meaning and influence readers in many domains. They have fostered students' interest in science and aided in knowledge retention (Negrete and Lartigue 2004). In political cartoons, comics were used to persuade readers toward a certain position through visual-textual metaphors and caricatures (Treanor and Mateas 2009). Comics were found to be effective at changing readers' attitudes, such as youths' attitudes toward mental health (Rose 1958). Health "graphic stories" (e.g., (Marchetto 2014)) were used to provide patients the means to learn about their illness while illustrating potential physical and emotional experiences through fictional characters and narrative. Medikidz (2016) created a series of comic books that teach children about common health conditions such as asthma and childhood obesity. In children's privacy education, a graphic novel by the The Office of the Privacy Commissioner of Canada (2016) tells the story of two siblings who encounter privacy risks related to social networking, mobile devices, and gaming. However, the comic has not been empirically evaluated for effectiveness.

People actively learn from comics because it is a form of multimodal text (Jacobs 2007). The juxtaposition of related text and images to convey information might be an appropriate learning format for children. Comics are motivating to read, visual, and permanent (in contrast to "time-bound" media like film or animation), and popular among children and youth (Yang 2016). They could be used as an intermediate step to learn about difficult subjects and concepts (Yang 2016), such as computer security and privacy. For example, comics that present stories about interrelated privacy consequences were proposed to simplify complex privacy notices (Knijnenburg and Cherry 2016). In one study, adults who received comic strip interventions performed better than text/graphic interventions (Kumaraguru et al. 2007). Other studies with adults found that comics improved security understanding and motivated positive changes in security management behaviour (Zhang-Kennedy et al. 2014, 2016). Srikwan and Jakobsson (2008) suggest that this is because online comics offer greater accessibility and immersion in the material than traditional security education efforts.

As up to ninety-nine percent of 9- to 16-year-old Canadian children go online using mobile phones, there is a need to teach them practical skills to protect their privacy (Steeves 2012). Although Secure Comics was initially created with a general audience in mind, the content, format, and literacy level also seem appropriate for children 11 years and older. This age group is capable of abstract and logical thinking, and have developed reasonable literacy skills (Piaget 2002). They are capable of imagining scenarios and think about the possible consequences of a situation (Piaget 2002).

3. SECURE COMICS

Secure Comics is a three-part educational interactive digital comic book series created by us that had positive effects on adult users' understanding of security and privacy topics and security management behaviour (Zhang-Kennedy et al. 2016). This study focuses on the chapter that addresses the risks of mobile online privacy.

We first identified the lesson content and drafted a narrative script. Next, storyboards were developed and iterated based on constructive feedback from security and privacy researchers in our lab and other graphic designers. The comics were drawn and produced by us using Adobe Creative Suite graphics software and a Wacom graphics tablet, and implemented in GameSalad Creator[1] to create the interactive features. We give an outline of the characters, narrative, and interactive features.

Characters: Jack and Nina are cyber-detectives who solve computer security crimes to protect the public from the cyber-villain "Hack". They act as mentors to teach users about various risks and protection strategies. Minor characters are introduced in the comic to support the overarching narrative.

Privacy Chapter Narrative Summary: Agent Jack takes a picture and uploads it online. He admits that taking pictures with smartphones is fun and convenient, but cautions that location-based data are automatically tagged to photos in a process called geo-tagging. The cyber-villain Hack is able to extract many types of user information from pictures. Indeed, his recent victim is a woman named Jane, who revealed many secrets through photos posted online (See Figures 1, C & D). Nina and Jack explain online tracking and how to prevent it.

Interactive Features: The privacy chapter has nine screens, three of which contain interactive features. First, users could tap on the camera icons over geo-tagged photos in the "Geo-tagging" screen to show metadata information (See Figure 1, B). Second, users could interact with an activity map on the "A day in the life of Jane" screen to show possible consequences of photos sharing (See Figure 1, D). Lastly, the comic concludes with a drag-and-drop mini quiz game that provides textual feedback to help users review the key concepts.

We applied instructional design principles (ID) (Gagne et al. 2005) to the comic design (the principles are summarized in Table 1). We used the *segmenting* principle to include one topic per chapter as Agents Jack and Nina tackle a new security crime committed by Hack. Each comic is divided into sections and pages to enable users to progress at their own pace. Interactive components showing cause and effect relationships encourage *reflection* on the *contiguous* images and text. The mini quiz-game at the end of the comic incorporates the principle of *immediate feedback* when users answer a question. The comic uses positive and conversational language (i.e., *personalization*). The use of colour over a monochromatic interface is designed to *signal* users' attention to important elements on the page. We applied the *multimedia* principle through juxtaposition of text, images, and interactive elements to create interest and reduce the cognitive load. Lastly, the comic helps users develop *conceptual knowledge* by building mental models through metaphors and telling analogies, then provides *procedural* examples to help reinforce the concepts. The current study with children extends our previously published work (Zhang-Kennedy et al. 2016) with adult users, where more details about the design process is described. Secure Comics is available online (CHORUS Lab 2017).

4. METHODOLOGY

In our two-session between-subject study, the dependent variables are *privacy knowledge* and *privacy behaviour*, and the independent variable is the type of media (i.e., the comic or the same narrative text-only presentation). In our study, we used children's responses to situation-based scenarios as a proxy for real behaviour. The scenarios were created as realistically as possible with circumstances relevant to children. Furthermore, the questions were framed objectively with a clear context. In privacy and security research,

[1] GameSalad Creator is a development toolkit for making interactive games.

ID Principles	Description	Implementation
Segmenting	Segment information into learner-paced chunks to give users opportunities to pause, process, and reflect before continuing to the next step.	The comic is segmented into sections and pages to enable users to progress at their own pace. Users press a forward or backward button to move ahead or backtrack.
Contiguity	Present words and corresponding images contiguously to increase learning performance.	Graphics are designed to complement text explanations and facilitate comprehension.
Reflection	Provide users with opportunities to reflect on what they learned to increase learning.	Interactive components in the comic cue reflection of the lesson content by concealing answers under graphics that are activated on mouseover.
Immediate Feedback	Provide immediate feedback helps users to assess how they are doing.	Users receive constructive immediate feedback in the mini-quiz game about why their choices are correct or incorrect.
Signaling	Direct user attention to key messages in the lesson to help with information discovery and understanding.	Various visual treatments (e.g., bold, colour-highlighting) are applied to text and graphical information to direct the learners' attention.
Personalization	Attribute social characteristics to the user interface that resemble human-to-human interaction help to engage users.	Jack and Nina guide users through the lesson and motivate users along the way. They use a positive conversational language when speaking to users.
Multimedia	Use words and graphics to increase learning rather than just text or graphics alone.	Ideas are expressed through text, images, and interactive elements to engage users.
Conceptual-Procedural	Show causal relationships between conceptual knowledge (e.g., mental representation of an idea) and procedural knowledge (e.g., steps to solve a problem or complete a task)	The comic helps users develop conceptual knowledge by building mental models through metaphors and telling analogies (e.g., "trail" metaphor), and provide procedural examples to help reinforce the concepts.

Table 1: *Instructional Design principles used in Secure Comics*

measurements of real behaviour are often unethical and sometimes not possible without putting users in compromising situations. This issue is particularly sensitive when the participants are children. As an alternative, measurements of intent have been accepted as a reasonable proxy for behaviour in usable security literature (Egelman and Peer 2015).

The study is based on a between-subject pre-test, post-test, followup (PPF) design commonly used to study intervention effects in child and adolescent research (Rausch et al. 2003). In PPF design, the dependent variable is measured on three separate occasions to determine if an effect exists and persists after the end of the intervention (Rausch et al. 2003). The dependent variable is first measured prior to intervention to establish a baseline, immediately after the intervention, and finally at a specified time after the end of the intervention. In our study, the followup is conducted after one week. A week interval is often used in recognition and recall based lab studies such as authentication (e.g., (Dhamija and Perrig 2000; Chiasson et al. 2007)). The time frame was also reasonable for scheduling with busy families.

Our research questions were: 1) Do the groups differ in privacy knowledge and behaviour from the pre-test to the post-test? 2) Do the groups differ in privacy knowledge and behaviour from the pre-test to the one-week-test? 3) Do the groups differ in privacy knowledge and behaviour from the post-test to the one-week-test?

Text control: We selected text as the control condition because users typically read privacy and security information online through various types of textual communication such as privacy policies, warning dialogue boxes, and advice columns. The format also enables us to isolate the information content to its most basic form by striping away all visuals, audio, and interactivity. Even though other methods are possible, they had limitations for our study. For example, it would be difficult to control for variability in a real-time lecture delivered by a teacher. Other time-bound media such as a filmed lecture or an instructional video reduces variability, but the content may need to be altered for adaptation to film. Furthermore, films are passively "watched", whereas comics and text need to be actively "read". Based on these considerations, text was the most appropriate control for our comic study.

The same-narrative text-only control condition was designed to read like a children's storybook and replicated the same narrative flow as the comic. All textual information was retained from the comic. To compensate for the lack of visuals, we added scene descriptions and other descriptive textual information to create a comparable reading experience as the comic. For example, children who participated in the *Comic* procedure read the screen shown in Figure 1, B, while children who participated in the *Text* procedure read the following text segment:

> "Pictures taken by most smartphones automatically attach location based data called geo-tagging," Jack continued. "Geo-tagging photos is a useful feature on the Internet, allowing people to share the location of experiences through their photos, such as where you took a picture of a sunset, an awesome event, or the location of that amazing restaurant you tried!"
> "On the flip side", Jack cautioned, "there is a risk of online tracking with geo-tagged photos." Jack pulls out a picture of dreamy beach sunset, a lively concert photo, and a picture of a delicious-looking plate of sushi. Upon closer inspection, the three photos displayed the following information:

IMG_3857.jpg Location: Cancún, Mexico Date: December 21, 2013 Time: 5:10pm Latitude: 21.1606° N Longitude: 86.8475° W
IMG_2457.jpg Location: Montreal, Canada Date: January 2, 2014 Time: 8:56pm Latitude: 45.5000° N Longitude: 73.5667° W
IMG_7584.jpg Location: Toronto, Canada Date: March 11, 2014 Time: 7:17pm Latitude: 43.7000° N Longitude: 79.4000° W

The *Comic* group read Secure Comics on iPads; the *Text* group read on 8.5" by 11" printouts. Families were provided with 2 iPads or 2 printouts and chose to read together or independently for as long as they liked. Most child-parent pairs chose to read independently. Children took on average 10 minutes and 50 seconds to read the *Comic* and 9 minutes and 40 seconds to read the *Text*. Session-I took 40 minutes, and Session-II took 20 minutes overall.

4.1. Participants and Recruitment

Twenty-two children between the ages of 11 to 13 (10 male, 12 female, mean age = 11.9 yrs) participated in our REB approved study. Most were accompanied by mothers (one by a father). The parents were between the ages of 30 to 49 from a wide range of education and economic backgrounds, including a bachelor's degree (*n* = 13), college diploma (*n* = 3), high school diploma (*n* = 3), and graduate degrees (*n* = 3). Six mothers were stay-at-home moms; others worked in education (*n* = 6), social services (*n* = 1), business (*n* = 4), and healthcare (*n* = 5). All children regularly used a mobile device. Their main activities were Youtube (22/22), app-games (21), picture-taking (19), web-games (16), web browsing (16), messaging (16), music (15), and Netflix (15).

To recruit families, we posted announcements on local parenting groups on Facebook. The Facebook groups were public and anyone could post to share news, local events, and other types of information. Additionally, we contacted local education resource centers who forwarded our recruitment notice to parents on their email mailing lists. Parents signed informed consent forms, and the children gave verbal assent. Each family received a $20 honorarium. The participants were identified by codenames preserving the child-parent pair. For example, C1-comic is read as "child 1, comic condition", P2-text is read as "Parent 2, text condition", and C1-comic is the child of P1-comic. Child participants were pseudo-randomly assigned to either the *Comic* (M = 5, F = 6, mean age = 12.1) or *Text* condition (M = 5, F = 6, mean age = 11.6) but gender was balanced between conditions to avoid gender effects.

4.2. Evaluation Measures

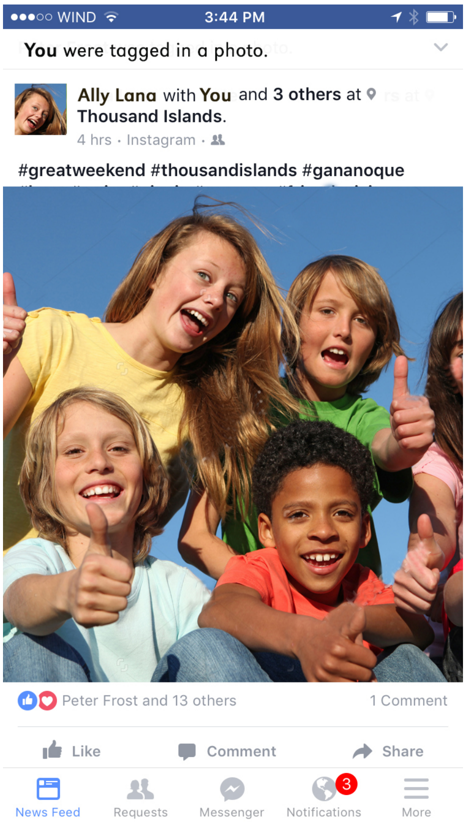
In the following section, the evaluation measures are labelled according to the letter code listed in the study procedure in Table 2.

A) Demographic/Activities, Pre-Evaluation Questionnaires: All parents completed an Adult Demographic Questionnaire (age, gender, education, and occupation), and a Child Demographic (age, gender, grade) & Activities Questionnaire (children's daily device use duration and going online, types of devices, online activities. and whether children had prior privacy/safety education). The Pre-Evaluation Questionnaire for parents was intended to assess whether they have a dominant criteria for choosing educational apps for kids. Parents ranked the criteria "fun", "age-appropriateness", "ease of use", "educational value", and "effectiveness" from rank 1 (most important), to rank 5 (least important) .

B) Children's Privacy Tests: The tests included ten knowledge-based questions and four behaviour-based scenarios. To evaluate users' computer security and privacy intention and practices, we assess both knowledge and behavioural aspects. To measure *privacy knowledge*, children recalled information learned from the narrative (e.g., "what is online tracking?") and made inferences (e.g., "How does your smartphone track your location?"). To measure *privacy behaviour*, children responded to

Procedure & Materials			
Ses.	**Participants**	**Comic Procedure**	**Text Procedure**
I	Parent	A) Demographic Questionnaires	A) Demographic Questionnaires
	Child	B) Pre-Test Interviews	B) Pre-Test Interviews
	Parent&Child	Read *Comic*	Read *Text*
	Parent	C) Adult Usability Questionnaire	N/A
	Child	C) Child Usability Questionnaire	
		B) Post-Test Interviews	B) Post-Test Interviews
1-week Interval			
II	Child	B) 1-Week-Test Interviews	B) 1-Week-Test Interviews
	Parent&Child	N/A	Read *Comic*
	Parent		C) Adult Usability Questionnaire
	Child		C) Child Usability Questionnaire

Table 2: *Summary of the study procedure. Materials are described in Section 4.2. The colours group similar activities together.*



You were tagged in a photo.

Ally Lana with **You** and **3 others** at **Thousand Islands.**

4 hrs · Instagram ·

#greatweekend #thousandislands #gananoque

Peter Frost and 13 others

1 Comment

Figure 2: *An example of the supplementary visual aids used with the scenarios in both conditions.*

scenarios presented with visual aids. For example, children saw a screen capture of a social media post (see Figure 2) and read the following situation: "you took a group picture with your friends on a trip and one of them asked you to post the picture online, check-in your location, and tag everyone in it". Children explained what they would do and how the situation might affect their own and others' privacy. The pre-tests established a baseline for each child, and the questions were repeated verbatim in the post-tests. The 1-week-tests evaluated the same concepts but contained alternate scenarios.

C) Child & Parent Usability Questionnaire: All participants completed a usability evaluation of Secure Comics. We wanted to make the study experience fun for families by allowing the *Text* group to also experience Secure Comics and complete a usability evaluation. The study procedure was designed to not confound other study measurements by having the *Text* group view and evaluate Secure Comics only after they completed the privacy tests (see Table 2). To check for possible bias caused by the *Text* group having previously read of the text-only format, we conducted Mann-Whitney U tests; they indicate that viewing order had no effects on children's opinions of the comic (Engagement: $U = 47.50, Z = -.97, p = .33$; Ease of Use: $U = 49.00, Z = -.84, p = .40$; Ease of Learning: $U = 55.00, Z = -.39, p = .70$). No significant differences were found between the conditions.

The child questionnaire contained eight questions. Engagement was measured using an Again-Again Table (Read and MacFarlane 2006) asking: *1) Would you read the comic book again?* (coded 3 for "yes", 2 for "maybe" and 1 for "no"). The next five questions used the Smileyometer (Read and MacFarlane 2006) (i.e., visual Likert-scales; 1 = least positive, 5 = most positive) to elicit opinions on the following: *2) How fun was the comic book? 3) How easy was it to use the comic book? 4) How well did you learn from the comic book? 5) How likeable were the characters? 6) How willing would you be to show the comic book to other kids?* The last two are open-ended questions that asked: *7) What did you like about the comic book? 8) What did you dislike about the comic book?* The parent version tested the same constructs using regular Likert-scales.

4.3. Interview Data Analysis

The transcribed interviews from audio recordings were organized in Excel into responses according to the interview questions. A researcher coded each of the participants' response (3 = very good, 2.5 = good, 2 = marginal, 1.5 = poor, 1 = very poor), for a total out of 30 for *privacy knowledge*, and 36 for *privacy behaviour*. A second researcher independently coded 50% of the responses. A Cohen's Kappa (k) test showed strong agreement between the two researchers' analysis of the pre-test ($k = 0.9$, 95% CI: $.8$ to $.9$, $p < .001$), Post-test ($k = 0.8$, 95% CI: 0.7 to 0.9, $p < .001$), and 1-week-test ($k = 0.8$, 95% CI: 0.7 to 0.9, $p < .001$). In cases of disagreement, the two researchers discussed and consolidated the final scores.

5. RESULTS

We compared children's knowledge and behaviour scores on three separate occasions during the study: pre-test, immediately after reading (post-test), and one week later. As recommended by Rausch et al. Rausch et al. (2003), we used one-way Analysis of Covariance (ANCOVA) tests to detect differences between groups in the post- and 1-week-tests using children's pre-test scores as a covariate to control for their pre-existing knowledge and behaviour. Furthermore, we tested children's 1-week privacy scores between the two conditions after controlling for their learned knowledge and behaviour using children's post-test scores as a covariate. The results are summarized in Table 3 and visualized in Figure 3. The unadjusted and adjusted means used in the analysis are summarized in Table 4.

The assumptions for the ANCOVA were met, including linearity, homogeneity of regression slopes, normality, homoscedasticity, and homogeneity of variances. One outlier in the knowledge post-test data of the *Text* condition and one outlier in the 1-week-test behaviour data of the *Comic* condition were replaced with the next lowest values in the group, as is standard practice.

5.1. Effects on Privacy Knowledge

Taking children's pre-existing knowledge (pre-test) into consideration, we found no statistically significant difference between conditions for their post-test scores. Analysis of the 1-week-test scores however, showed a statistically significant difference between the conditions in privacy knowledge, $F(1, 19) = 18.5$, $p < .001$, partial $\eta^2 = .493$. The mean scores of the 1-week-test were adjusted by the covariate (pre-test) from 26.8 to 26.6 points for *Comic*, and from 22.5 to 22.6 points for *Text*. Post hoc analysis showed that 1-week privacy knowledge was greater in the *Comic* group than in the *Text* group. Further analysis of the post- vs. 1-week tests also showed a significant difference between groups, $F(1, 19) = 12.8$, $p = .002$, partial $\eta^2 = .403$. Specifically, the *Comic* was significantly more successful than *Text* at sustaining privacy knowledge after one week.

Privacy Knowledge			
Tests	MD	95% CI	p
Pre/Post	1.8	[-.3, 3.9]	.090
Pre/1-week	4.0	[2.0, 6.0]	**.001**
Post/1-week	3.1	[1.3, 5.0]	**.002**
Privacy Behaviour			
Pre/Post	2.2	[.5, 4.0]	**.013**
Pre/1-week	3.8	[.8, 7.0]	**.016**
Post/1-week	2.0	[-1.9, 6.0]	.304

Table 3: *ANCOVA tests showing statistically significant differences between groups for* privacy knowledge *in the Pre/1-Week-Test and the Post/1-Week-Test. A statistically significant difference between groups for* privacy behaviour *was found in the Pre/Post-Test and the Pre/1-Week-Test.* MD *= Mean Difference,* CI *= Confidence Interval,* p *= Significance Level.*

5.2. Effects on Privacy Behaviour

Children's pre-existing behaviour assessed by their pre-test scores was used in the analysis. We found a statistically significant difference between groups immediately after reading, $F(1, 19) = 7.5$, $p = .013$, partial $\eta^2 = .284$, and one week after reading $F(1, 19) = 7.0$, $p = .016$, partial $\eta^2 = .270$. Post-test mean scores were adjusted by the covariate (pre-test) from 32.0 to 31.9 points for *Comic*, and from 29.5 to 29.7 points for *Text*. 1-week-test mean scores were adjusted by the covariate from 31.1 to 31.0 points for *Comic*, and from 27.2 to 27.3 points for *Text*. Post hoc tests showed the *Comic* was more successful at influencing children's post-test and 1-week-test privacy behaviour than *Text*.

5.3. Results Summary

Both conditions improved children's privacy knowledge immediately after reading and after one week. Both conditions also improved children's privacy behaviour immediately after reading. However, after one week, children who read the comic were significantly more likely to chose privacy-preserving behaviours. Those in the *Comic* condition showed greater increases in their privacy knowledge and behaviour scores, and maintained higher scores after one week, even when adjusted for variance in baseline knowledge and behaviour. The comic appears more effective than the text-only format at conveying knowledge and persuading children to consider privacy-preserving behaviours.

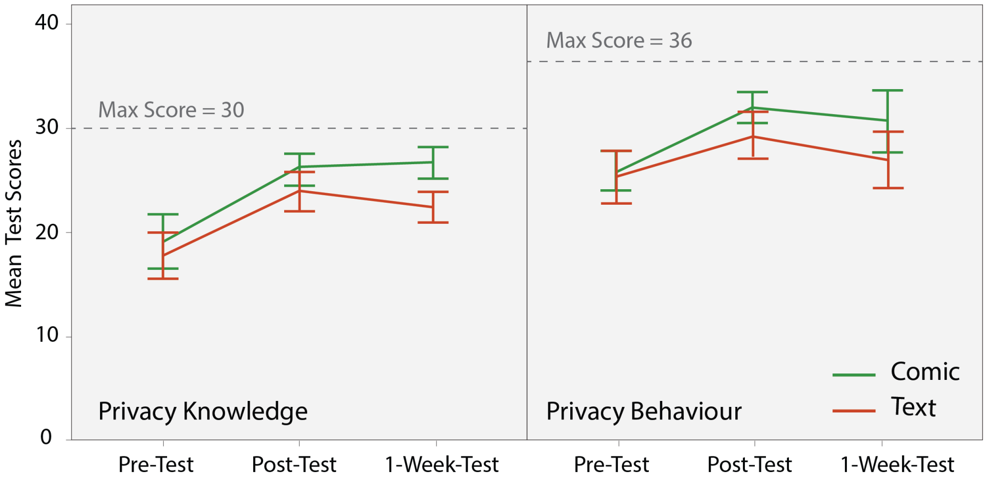


Figure 3: *Children's privacy knowledge and behaviour over time between groups. Error Bars: 95% Confidence Interval (CI)*

Privacy Knowledge						*Privacy Behaviour*			
		Unadjusted		Adjusted		Unadjusted		Adjusted	
Tests	Condition	M	SD	M	SE	M	SD	M	SE
Pre/Post	Comic	26.2	2.3	26.0	.7	14.5	2.6	14.1	.5
	Text	24.0	2.8	24.2	.7	13.5	2.7	13.9	.5
Pre/1-Week	Comic	26.8	2.3	26.6	.7	15.4	1.8	15.2	.4
	Text	22.5	2.2	22.6	.7	13.0	1.7	13.3	.4
Post/1-Week	Comic	26.8	2.3	26.2	.6	15.4	1.8	15.2	.4
	Text	22.5	2.2	23.0	.6	13.0	1.7	13.3	.4

Table 4: *Adjusted and unadjusted means and variability for the Post-Test and 1-Week-Test privacy proficiency scores with Pre-Test privacy proficiency scores as a covariate, and 1-Week-Test privacy proficiency scores with Post-Test privacy proficiency scores as a covariate. Adjusted means are used in the analysis. M = Mean, SD = Standard Deviation, SE = Standard Error.*

6. USABILITY OF SECURE COMICS

Figure 4 shows children's opinions on engagement, ease of use, and ease of learning for the comic.

Secure Comics is engaging: Children's assessment of whether they would like to repeat the activity is highly correlated to engagement (Read and MacFarlane 2006). The Again-Again evaluations showed that more than half of children are confident that they would read Secure Comics again ("yes" n = 13, "maybe" n = 9, "no" n = 0). Furthermore, their Smileyometer evaluations showed a mean of 4/5 for "fun". Children said the learning experience was fun because of the graphical format and interactivity, and because the information is told through a story. C7-Comic thought the comic was "fun and interactive". C6-Text thought the comic "was funny". C1-Text "liked the graphic format and being able to interact with the comic". C3-Comic "liked the characters", and C2-Text thought "the drawings were cool". Children suggested additional character information, less text, more colour and interactive challenges.

Secure Comics is easy to use: Children thought the interface was very ease to use (Mean = 4.3/5). The only difficulty we observed was the drag-and-drop quiz feature, where children preferred to tap. Some found certain "big words" difficult to understand like "geo-tagging".

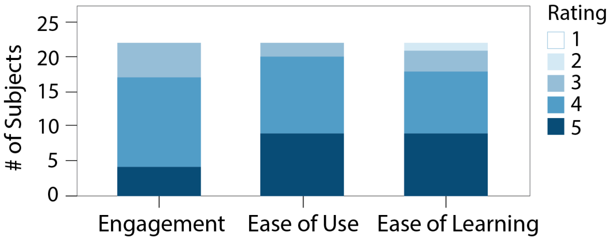


Figure 4: *Summary of children's usability evaluations (5 = most positive).*

Secure Comics made learning easy: Children felt they learned well (Mean = 4.2/5). C10-Text said, "a lot of people use electronics without caring. The comic helps people care more about their privacy." C3-Text felt "there was a lot of information, but it was split up well." C2-Comic liked "the different situations that could be relatable for people."

6.1. Parents' feedback

Parents' pre-evaluation rankings of criteria in choosing an educational app for 11- to 13-year-old children showed that they had varying opinions. The rankings averaged at 2.5 (rank 1 = most important) for *educational value*, 2.6 for *effectiveness*, and 2.9 for *age-appropriateness*. It seemed that *fun* (3.4) and *ease of use* (3.6) were the least important criteria.

Parents' post-evaluation of the comic was consistently positive, with 4.6/5 for *educational value*, 4.5 for *effectiveness*, 4.4 for *age-appropriateness*, 4.0 for *fun*, and 4.6 for *ease of use*. Parents felt that the comic "used real-life situations, which facilitated discussion points and made the topic very relevant"; "The presentation is interactive and interesting, and it seemed less like "work" to review with [their] child" (P3-Text). They felt the format was age-appropriate: it "helped [my child] learn more about privacy while doing this in a fun and gentle format. (P4-Comic); Another parent said, "I liked that it explained a complicated and somewhat scary topic in a fun and easy to use way. I found 'A day in the life of Jane' very effective in showing how a hacker can track your movements throughout the day" (P3-Comic). To improve, parents suggested brighter colours, a deeper story, and more interactive features.

7. DISCUSSION

Turner and Harviainen (2016) suggest that users pretend and make-believe when they *act though* or behave *as if*. Unlike pretending however, make-believe relies on props such as a good story or an artifact to act on a make-believe episode (Walton 1990). Our study showed that storytelling through a comic narrative acted as an effective prop for children to learn and retain privacy information after one week, suggesting that it is superior to text-narratives for supporting children's short and long-term knowledge retention and behaviour.

7.1. Supporting Children's Memory

Our study found that both narrative formats supported children's short-term memory, but a visually rich comic was more successful than the text narrative at supporting knowledge retention. Working memory stores information in the short term, which can be retrieved to coordinate perception, long-term memory, and action (Schmidt and Bjork 1992). Long-term memory retrieves information by consciously recalling previous experiences or known facts (Schmidt and Bjork 1992). The comic narrative had superior immediate and 1-week effects on children's privacy knowledge and behaviour than the text narrative. After one week, the *Comic* group maintained the learned knowledge while the *Text* group forgot some of the knowledge learned. The result supports Dual-Coding Theory that states the combination of related text and images increase long-term memory (Paivio 1991). This result is also consistent with our previous study with adults (Zhang-Kennedy et al. 2016), where participants showed an excellent retention of knowledge post-test and one week later.

7.2. Persuading Privacy-Conscious Behaviour

We found the visually rich comic narrative is more effective at driving behaviour change than the text narrative. Children's response to situation-based scenarios dramatically improved after they read the comic. After one week, the *Comic* group maintained privacy-conscious behaviour while the *Text* group showed a decrease in desired behaviour. This suggests that the comic was more successful at sustaining changes in children's behaviour after one week. Positive behaviour change was also reported in our adult study (Zhang-Kennedy et al. 2016).

Several factors unique to children's behaviour were taken into consideration in this study. First, children are still developing new experiences with technology, and second, parents share the responsibility for managing their privacy and security. It is therefore impractical to expect certain behaviour from children, such as changing location-based settings on their smartphones, because some may not own a smartphone (e.g., they borrow their parents') or they do not have access to the activity that could put them at risk (e.g., they are too young to have social media and post pictures). These factors influence children's behaviour and could change over time. Teaching appropriate behaviours and helping them become privacy-aware can help persuade them towards more independent privacy-conscious actions.

7.3. Child-Centered Privacy/Security Education

Privacy and security education has several unique challenges that could be addressed through interactive comics. First, persuading children to behave in a privacy-preserving manner is difficult because, like adults, they typically do not regard privacy and security as primary concerns (Whitten and Tygar 1999), because their main use of mobile devices is for entertainment (Steeves 2012).

Our study showed that children found Secure Comics very engaging and fun. According to the ICAP hypothesis (Chi and Wylie 2014) for differentiating four levels of cognitive engagement (interactive, constructive, active, and passive), learning will increase as learners become more cognitively engaged with the learning material. Secure Comics supported passive and active learning. In passive modes of engagement, such as reading static text, learners receive the information from the instructional material without overtly doing anything else learning related. In active modes of engagement, learners partake in some form of overt motor action or physical manipulation. In Secure Comics, active learning was achieved by physically manipulating the interactive features and navigating between screens. The ICAP hypothesis therefore, suggests that reading an interactive comic would be more engaging than reading static comics.

Second, security threats constantly change and evolve compared to other types of safety advice that is relatively unchanged over time, such as wearing a seatbelt. This makes it difficult to give children definitive protective advice. Privacy boundaries are also personal in nature, requiring individuals to chose how much they are willing to share. Educational material should, therefore, aim to teach critical-thinking and ensure that children understand the potential consequences and tradeoffs of sharing information (Steeves 2012), rather than giving declarative rules that everyone must follow.

Comics are an adaptable media where content could be created more quickly to address new threats and at relatively low cost compared to other media types (e.g., animation, games). Families expressed interest reading the other existing chapters in Secure Comics, showing the potential of adding new educational content to the series in the future.

Third, users rely on mental models[2] to make privacy and security decisions. Children have poor mental models of privacy that are even less developed than adults' (Zhang-Kennedy et al. 2016) and this could have negative consequences on their protection behaviour. Secure comics use narrative storytelling, simple textual explanations, and graphics to illustrate complex privacy and security concepts. Children who read Secure Comics demonstrated careful, logical, and conscious thinking about different scenarios in the post- and 1-week-tests and acted in a more privacy-preserving manner on both occasions compared to the control condition. This suggests that comics helped children to develop richer mental models than textual information, which had positive influences on their privacy behaviour.

As children operate computers in different contexts than adults, and have different privacy concerns, there is a need for child-centred privacy and security solutions (Dempsey et al. 2016). Swan (2000) suggests that children's education should include digital literacy around using digital tools, critical literacy around interpreting and assessing information, and content literacy relating to composing and developing content. Our educational material focuses primarily on critical literacy. We believe that children should be given opportunities to develop the critical thinking skills and experience required to be aware and responsible digital citizens. Parental monitoring has its place and the degree of responsibility accorded to children will vary depending on the developmental stage of each individual child, but the aim should be to encourage learning appropriate actions for their given circumstances. We feel that our empirically-tested Secure Comics is a useful educational tool to aid in this process.

7.4. Limitations and Future work

Our scenario-based lab assessments of children's behaviour are used as a proxy for real life behaviour due to ethical concerns of putting children in compromising online situations. Although a promising approach, children's responses to scenarios may not directly translate to real life behaviour. Our 1-week study provided some indication of the long-term educational effects, and could be extended in a future longitudinal study. Our results may only be applicable for children 11 years and older due to younger children's developing working and long-term memory capabilities (Dempster 1981). In connection to recent trends in digital storytelling, our future work explores the interactive narrative format further in a children's interactive ebook that includes more multimedia features such as sound and animation, and support for co-use with parents.

8. CONCLUSION

As mobile technology becomes more prevalent among children, they need to learn about safe online interactions. We found that our comic is effective for increasing children's privacy knowledge and persuading them towards privacy-conscious behaviour. Children showed excellent learning effects and retention, especially considering that privacy concepts are complex and difficult to learn even for adults. They demonstrated significant improvements from their prior privacy behaviour, and were able to sustain the behaviour after one week. Children and parents found the comic easy to learn for children, engaging, and easy to use, showing that it is an appropriate education format for children. In conclusion, our research showed text-only narratives may be immediately effective for improving children's knowledge and behaviour, but vivid narratives like comics have more potential to maintain these persuasive effects in the long-term.

[2] A *mental model* is a simplified internal concept of how something works in the real world (Craik and Williams 1967).

9. ACKNOWLEDGMENTS

This project has been partially funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC. Sonia Chiasson acknowledges funding from NSERC for her Canada Research Chair in Human Oriented Computer Security.

REFERENCES

Chi, M. T. and R. Wylie (2014). The ICAP framework: Linking cognitive engagement to active learning outcomes. *Educational Psychologist 49*(4), 219–243.

Chiasson, S., P. C. van Oorschot, and R. Biddle (2007). Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security*, pp. 359–374. Springer.

CHORUS Lab (2017). Secure Comics. `http://versipass.com/edusec/securecomics`.

Craik, K. and J. Williams (1967). *The nature of explanation*, Volume 445. CUP Archive.

Dempsey, J., B. Cassidy, and G. Sim (2016). Child-centered security. In *British HCI*. BCS e-WIC.

Dempster, F. N. (1981). Memory span: Sources of individual and developmental differences. *Psychological Bulletin 89*(1), 63.

Dhamija, R. and A. Perrig (2000). Déja vu – a user study: Using images for authentication. In *USENIX Security Symposium*, Volume 9, pp. 1–4.

Egelman, S. and E. Peer (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Human Factors in Computing Systems*, pp. 2873–2882. ACM.

Friedland, G. and R. Sommer (2010). Cybercasing the joint: On the privacy implications of geotagging. In *USENIX Workshop on Hot Topics in Security*.

Gagne, R. M., W. W. Wager, K. C. Golas, J. M. Keller, and J. D. Russell (2005). *Principles of instructional design*. Wiley Online Library.

Hughes, F. P. (2009). *Children, play, and development*. Sage.

Jacobs, D. (2007). More than words: Comics as a means of teaching multiple literacies. *English Journal*, 19–25.

Knijnenburg, B. and D. Cherry (2016). Comics as a medium for privacy notices. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association.

Kumaraguru, P., Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor, and J. Hong (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *APWG eCrime Summit*, pp. 70–81. ACM.

Leslie, A. M. (1987). Pretense and representation: The origins of "theory of mind.". *Psychological review 94*(4), 412.

Marchetto, M. A. (2014). *Cancer vixen: A true story*. Pantheon.

Medikidz (2016, Accessed September). Medikidz: Medical information for kids. `http://www.medikidz.com/gb-en/`.

Negrete, A. and C. Lartigue (2004). Learning from education to communicate science as a good story. *Endeavour 28*(3), 120–124.

Paivio, A. (1991). Dual coding theory: Retrospect and current status. *Canadian Journal of Psychology 45*(3), 255.

Piaget, J. (2002). *Judgement and reasoning in the child*. Routledge.

Rausch, J. R., S. E. Maxwell, and K. Kelley (2003). Analytic methods for questions pertaining to a randomized pretest, posttest, follow-up design. *Journal of Clinical Child and Adolescent Psychology 32*(3), 467–486.

Read, J. C. and S. MacFarlane (2006). Using the fun toolkit and other survey methods to gather opinions in child computer interaction. In *Interaction Design and Children*, pp. 81–88. ACM.

Rose, A. M. (1958). Mental health attitudes of youth as influenced by a comic strip. *Journalism & Mass Communication Quarterly 35*(3), 333–342.

Schmidt, R. A. and R. A. Bjork (1992). New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training. *Psychological Science 3*(4), 207–217.

Sharples, M., R. Graber, C. Harrison, and K. Logan (2009). E-safety and web 2.0 for children aged 11–16. *Journal of Computer Assisted Learning 25*, 70–84.

Srikwan, S. and M. Jakobsson (2008). Using cartoons to teach internet security. *Cryptologia 32*(2), 137–154.

Steeves, V. (2012). Young Canadians in a wired world, phase III: Talking to youth and parents about life online.

Swan, K. (2000). Nonprint media and technology literacy standards for assessing technology integration. *Journal of Educational Computing Research 23*(1), 85–100.

The Office of the Privacy Commissioner of Canada (2016, Accessed September). Social Smarts: Privacy, the internet and you. `https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/social-smarts-privacy-the-internet-and-you/`.

Treanor, M. and M. Mateas (2009). Newsgames: Procedural rhetoric meets political cartoons. *Digital Games Research Association 2009*.

Turner, P. and J. T. Harviainen (2016). *Digital Make-Believe*. Springer International Publishing.

Walton, K. L. (1990). *Mimesis as make-believe: On the foundations of the representational arts*. Harvard University Press.

Whitten, A. and J. D. Tygar (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX Security Symposium*.

Yang, G. (2016, Accessed September). Comics in education. `http://www.humblecomics.com/comicsedu/index.html`.

Zhang-Kennedy, L., S. Chiasson, and R. Biddle (2014). Stop clicking on 'update later': Persuading users they need up-to-date antivirus protection. In *Persuasive Technology*, pp. 302–322. Springer.

Zhang-Kennedy, L., S. Chiasson, and R. Biddle (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction 32*(3), 215–257.

Zhang-Kennedy, L., C. Mekhail, Y. Abdelaziz, and S. Chiasson (2016). From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Interaction Design and Children*, pp. 388–399. ACM.