A Comic Authoring Tool for Enhancing Privacy and Security Lessons Through Informal Stories

Leah Zhang-Kennedy
University of Waterloo

Sangho Suh
University of Toronto

Abstract

Research shows that many people learn about privacy and security risks from anecdotal stories shared by others, which influence their perceptions and actions. However, no studies have been conducted with children, who may also gain significant knowledge about security and privacy from peers, trusted adults, and social networks. To promote the creation and sharing of privacy stories, we created PrivacyToon, a concept-driven storytelling tool that facilitates the visual production of privacy stories and visualizations. The tool provides users with creative and technical drawing support, where a comic story can be created, downloaded, and shared while improving the reflection of privacy issues in the process. A comic authoring tool centers users in the creation process to tell their own narratives that express their lived digital experiences or lessons from stories. We discuss our ongoing research on PrivacyToon and its potential as a security and privacy learning interface for children.

1 Introduction

Research [17, 18] acknowledges that many people learn about privacy and security risks from information derived from anecdotal stories shared by others, which could influence their corresponding actions. Although non-expert users appear to acquire knowledge about security through stories they hear from informal sources (e.g., family, friends, social media) [17, 18], no studies have been conducted with children. We hypothesize that stories from peers, trusted adults, and social networks also play a crucial role in children's "security and privacy education."

Our previous work [24] created a concept-driven storytelling tool called PrivacyToon[1] that facilitates the creation of privacy stories (see Figure 1 for examples). Sketching to elicit users' perceptions and understanding of privacy and security concepts has emerged as a subcategory of mental model-based research in usable privacy and security. The drawing elicitation method has been used to study various topics, such as non-experts and children's understanding of privacy [16], knowledge about how the Internet works [10], conceptions of online risks [8], and visual imagery for cybersecurity concepts [23] and warnings [5, 9].

PrivacyToon was the first online platform specifically created for privacy storytelling in the form of captivating comics. Although our previous research [28] found that comics have the potential to be a storytelling medium due to their visual and easy-to-digest format, the process of generating comics is time-consuming and not easily accessible. We therefore created PrivacyToon to address this limitation by providing users with creative and technical drawing support. A comic story can be created, downloaded (in PNG or SVG format), and shared quickly. The simplicity of the process of creating privacy stories enables us to imagine methods for effortlessly disseminating privacy and/or security narratives to enhance children's understanding of online risks. For example, a group of children in a classroom environment could share their online experiences and knowledge by creating short comic strips to prompt reflection and discussion.

Previous research in designing for children's privacy and security found that children's involvement in the design process is limited [13]. A comic authoring tool centers children in the creation process to tell their own stories and express their digital experiences. In this short paper, we describe our ongoing research of our authoring tool and dive into a discussion of its potential as a security and privacy learning interface for children.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

[1] https://privacytoon.github.io/

2 Background and Related Work

We highlight past research on the importance of anecdotal stories told to non-experts in forming their mental models and secure behaviors, point to gaps in the use of comics in cybersecurity education, and summarize the advantages of sketching as a methodology in usable privacy and security.

2.1 Stories as Informal Lessons About Security

According to previous research [17, 18, 25], people build their mental models of privacy and security threats by inferring information from informal stories told by others, which could influence their perception of security and the corresponding actions. For example, Rader et al. [18] discovered that narratives containing significant threats have an impact on cognitive processes and the probability of being recounted. According to Redmiles et al. [21], the primary origin of security advice is unpleasant incidents that participants have personally encountered or learned about from friends, family, and the media. Fennell et al. [7] discovered that narratives about security breaches heightened individuals' likelihood to embrace two-factor authentication. Based on these studies with adults, we hypothesize that children also gain a significant amount of their knowledge about online privacy and computer security from stories they hear from peers, trusted adults, and social networks. No previous research has investigated what kinds of stories children tell about security and privacy and how stories influence their online practices.

2.2 Comics for Cybersecurity Education

Security and privacy related comics exist in several formats for a variety of audiences [28], including comic strips (e.g., [22]) and interactive comics (e.g., [11, 11, 27, 29, 30]). Comics' visual storytelling capabilities could be an effective medium for communicating complex concepts of security and privacy concepts [22, 27, 29, 30]. However, the process of creating educational comics with current tools is laborious and time-consuming, where existing content could quickly become outdated [28]. Traditional comics also do not involve users as content creators in the process of generating information to effectively convey and contemplate their comprehension of security and privacy risks [24]. To fill this gap, our previous work, PrivacyToon [24], facilitates the rapid creation of privacy comics and visualizations with creativity support to aid users in producing comics that are more expressive and customized to their understanding of privacy. The narrative and pictorial characteristics of the comic medium can help strengthen users' mental models of privacy and facilitate the communication of privacy stories, as demonstrated in previous studies [22, 27, 29, 30].

2.3 Sketching Research Methodology

Researchers have proposed to identify mental models of privacy [16] and cybersecuirty [23] through illustration as a research tool to explore the visual culture of privacy and inform privacy-related visual design (e.g., iconography, risk communication). While traditional mental model research methodologies typically involve interviewing users to gain insight into how they perceive and respond to certain security concepts and software (e.g., [3, 19, 25]), sketching could offer additional insights into the expert and non-expert conceptualizations of abstract concepts that are difficult to express with verbal and textual information alone [2, 4]. For example, Oates et al. [16] utilized user-generated drawings to identify laypeople, privacy experts, children, and adults' mental models and metaphors of privacy, and found that experts' visual conceptualizations of privacy tend to depict online data spaces, while non-experts' drawings frequently illustrated public and private spaces in a physical context. Sturdee et al., [23] used a similar sketching method to analyze participants' understanding of cybersecurity concepts. Yao et al. [26] asked participants to brainstorm their desired ways to mitigate privacy issues and to draw their design ideas for smart home privacy mechanisms. Friedman et al. [8] used drawing tasks to illustrate the participants' understanding of web security, and found that people associated simple visual cues such as a lock icon and the presence of `HTTPS` with a secure connection. In a study by Kang et al. [10], insights about mental models of how the Internet works and the related privacy and security risks were also obtained by drawing conceptual diagrams. The drawing method is also useful for studies with vulnerable populations like and children (e.g., [5, 16]) and older adults (e.g., [20]), who might have difficulty articulating technical concepts through words. For example, Dempsey et al. [5] asked children to draw warning messages to inform design guidelines for privacy warnings tailored to children about information disclosure online.

Although sketching is a useful methodology that can visually capture user conceptualizations, people with poor artistic skills could feel uncomfortable drawing in free form using pen and paper and produce disparities in the level of drawing detail [20]. Through PrivacyToon, we addressed these limitations with a digital tool that facilitates the drawing process with creativity support (e.g., ideation cards) and technical drawing support (e.g., stencil library). The goal of the tool is to stimulate reflection about privacy concepts throughout the creation process. Providing assistance for creative thinking with respect to privacy is advantageous because privacy concepts can be complex and challenging to design for [13]. The interactive tool allows for unrestricted sketching and provides assistance in the process of *concept-driven storytelling* by guiding the creation of concepts, stories, and comic designs.

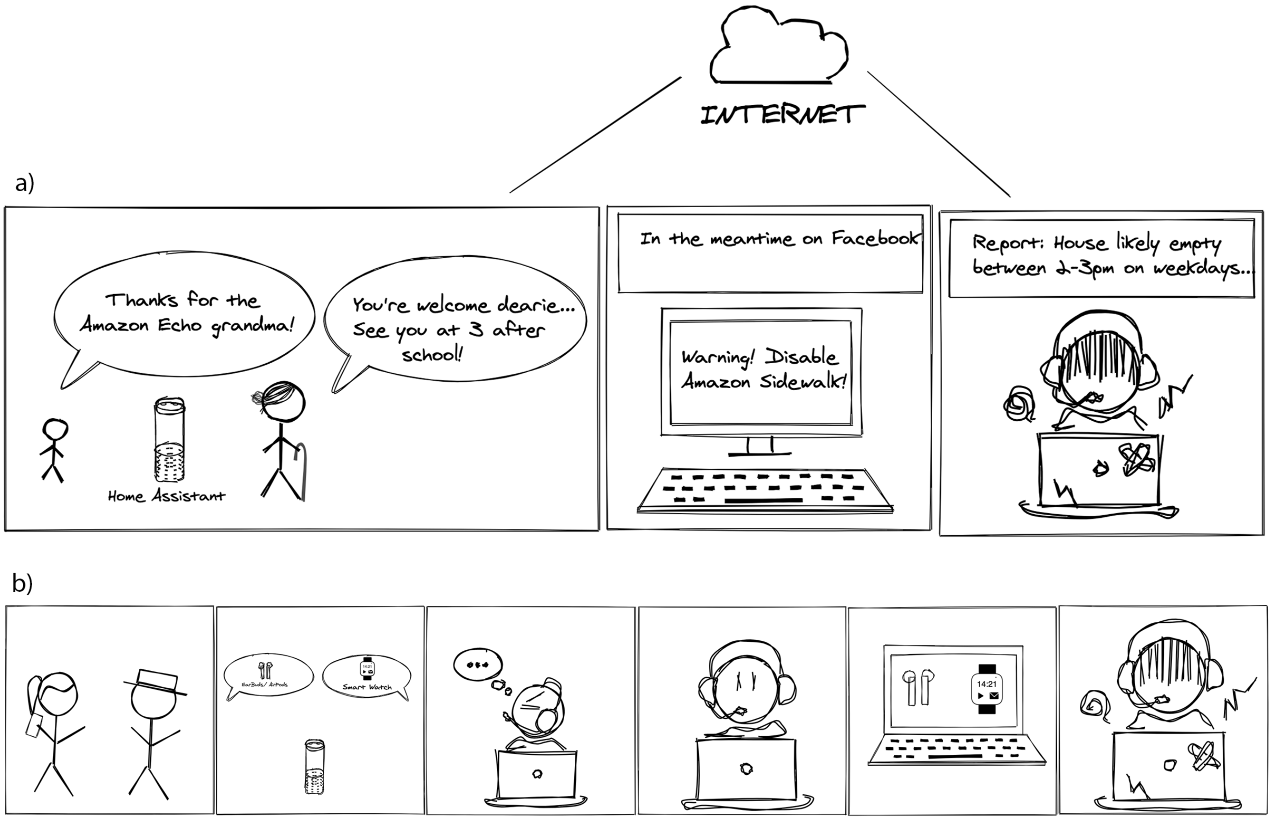
INTERNET
a)
Thanks for the Amazon Echo grandma!
You're welcome dearie... See you at 3 after school!
Home Assistant
In the meantime on Facebook
Warning! Disable Amazon Sidewalk!
Report: House likely empty between 2-3pm on weekdays...
b)
EarBuds/ AirPods
14:21
Smart Watch
14:21

Figure 1: The PrivacyToon tool supports free-style drawing and includes a stencil library to enable rapid authoring of comic strips. The figure shows participants' sample drawings using the tool from our ongoing work on IoT stories: a) A story heard from a friend warning about Amazon Sidewalk and how to disable it due to privacy concerns. b) A story heard from social media about Alexa's "always listening" capabilities for targeted advertising across devices.

2.4 Examples

We provide two motivating examples of novel storytelling enabled by PrivacyToon. In the first example, we explore stories related to sharing personal information online from students and teachers. In the second example, we investigated stories about the Internet of Things (IoT) that influence people's perceptions and adoption of smart home IoT devices. Although these examples do not focus on children, they aim to show the potential of our future work with children.

2.5 Example A: Stories About Sharing Personal Information Online

To evaluate PrivacyToon, we first conducted a user study [24] with 18 post-secondary students and 5 teachers who have taught at least one lesson related to security or online privacy at the high school, college, and university levels. For the purpose of demonstrating the storytelling aspect of the tool, we focus on our qualitative results of the comic content and design instead of the usability and utility of the tool.

We provided participants with excerpts from the Teaching Privacy curriculum[2], which was specifically designed for high school and undergraduate students, to establish a foundation of knowledge on the selected subjects: 1) exchanging information over a network, and 2) the concept of digital footprints that individuals leave online. We chose this resource based on its proven efficacy in teaching undergraduate students with non-CS backgrounds, as demonstrated in the study by Egelman et al. [6]. We collected 46 comic drawings depicting the two concepts using PrivacyToon from our participants, available online[3]. Our analysis showed that the participants used a wide range of graphic components derived from the stencil library and their own free-style drawings. For example, they used grin and angry emoji faces from the stencil library to symbolize feelings of "likes" and "dislikes". Participants often used metaphors and analogies in their comic creations, such as drawing a chocolate chip cookie to represent a "*HTTP*

[2] https://teachingprivacy.org
[3] https://privacytoon.github.io/download/

cookie" and using the word "oven" metaphorically to describe a browser. The comic samples exposed a variety of creative representations to explain privacy issues, such as stories that contained a lesson and showing cause-and-effect relationships (e.g., consequences of oversharing personal information online). Preliminary feedback from teachers suggests that the authoring tool could increase students' engagement in the classroom (e.g., through classroom activity and discussion) and allow teachers to supplement lessons with explanatory images that reinforce privacy and security concepts.

2.6 Example B: Stories about Smart Home IoT

In our work in progress, we examined whether stories shared by others that emphasize positive and negative experiences impact the trust and willingness of story recipients to use IoT devices, even if they have not personally experienced similar incidents described in the stories. Using the PrivacyToon tool, we collected 263 narratives about smart home IoT in an online survey. The participants provided a variety of anecdotes they had encountered with regard to IoT devices and selected a particular story that they could easily recall and share in the survey. They provided responses to a set of questions related to the source and location from which they heard the story, the level of seriousness of the event, and their belief in the truthfulness of the story. The participants then indicated the impact of the narrative they heard on their perceptions, trust, and willingness to use IoT devices.

Our preliminary data analysis showed a range of themes that individuals relate to IoT technology. Positive attitudes revolve around the advantages of using IoT devices for home monitoring and enhancing daily life, whereas negative sentiments usually refer to security breaches, surveillance, and the unreliability of IoT. Attitudes toward the types of device on which the stories focused aligned with these themes. For example, the participants recounted a greater number of favorable anecdotes about home security systems and unfavorable anecdotes about voice assistants (see Figure 1).

3 Discussion and Future Work

The ramifications of our investigation are intriguing in terms of differences in individuals' conceptions of privacy and attitudes toward certain types of technology. Due to the widespread dissemination of information and the amplification of narratives on social media and the Internet, people are regularly influenced by the tales they encounter, and we suspect that children are as well. Our future work proposes to investigate two aspects. First, we propose to use our tool to investigate stories that shape children's understanding and the ways in which these stories affect their actions. Second, we propose studies on the use of the tool to facilitate the learning of security and privacy concepts from stories created and shared by children in classroom settings.

Previous work [1, 12, 14, 15, 30] emphasized that security and privacy educational tools that enable exploration, foster critical thinking skills and reflection, and promote discussion are important design considerations. Our storytelling tool could support activities with children by incorporating stories and role-playing with scenarios. Scenarios in particular would be a powerful tool for learning about online privacy, as when students can see themselves in similar situations, they are more likely to learn from them and apply the lessons to situations in their real life [1]. Scenarios and role-playing are also known to help facilitate reflection, since by giving students the opportunity to reflect on their choices, they are able to grasp nuanced situations [14].

PrivacyToon could allow educators and students to create their own custom comic stories as a teaching and learning tool. For example, a teacher could supplement a privacy lesson with explanatory images created in PrivacyToon to streamline the creative process of producing visuals for a lesson. Likewise, a student could use the tool to create comics as a creative exercise to demonstrate their understanding of the lesson and share them with the class. The tool is scalable across different domains to cover other concepts because the ideation cards are customizable. The creativity support features offered within PrivacyToon in the form of ideation cards could serve as prompts about online risks as a way to increase children's awareness about the issues.

Children could create their own stories digitally or as printouts using the concept-driven storytelling process embedded in the tool and share them with classmates, family, and friends. Teachers could use PrivacyToon to facilitate discussions and classroom activities to engage students in critical thinking and reflection, either by explicitly outlining the major themes and topics on which the stories should focus on, ask students to create short comics about an online incident they experienced, or portray stories they heard from other people as a way to reflect on and learn from the incidents and risks in the story.

4 Conclusion

We proposed using the PrivacyToon comic authoring tool to study how stories can inform children's understanding of security and privacy concepts, and as a platform to create, reflect, and share their experiences or stories they heard from other people. Our research is grounded in research about ways people learn about privacy and security risks from anecdotal stories shared by others. After providing two motivating examples, we demonstrated how our tool has been used so far to understand people's interpretations of privacy lessons and attitudes towards IoT technology. These examples are meant as a starting point to motivate similar research approaches with children using our tool to learn about their understanding of online concepts and to study ways they learn about security and privacy risks through storytelling.

Acknowledgments

Zhang-Kennedy acknowledges funding support from the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grants.

References

[1] Elana B Blinder, Marshini Chetty, Jessica Vitak, Zoe Torok, Salina Fessehazion, Jason Yip, Jerry Alan Fails, Elizabeth Bonsignore, and Tamara Clegg. Evaluating the use of hypothetical 'would you rather' scenarios to discuss privacy and security concepts with children. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1):1–32, 2024.

[2] Flora Bowden, Dan Lockton, Rama Gheerawo, and Clare Brass. Drawing energy: Exploring perceptions of the invisible. 2015.

[3] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[4] Andrew Cox and Melanie Benson. Visual methods and quality in information behaviour research: The cases of photovoice and mental mapping. *Information Research: An International Electronic Journal*, 22(2):n2, 2017.

[5] John Dempsey, Gavin Sim, Brendan Cassidy, and Vinh-Thong Ta. Children designing privacy warnings: Informing a set of design guidelines. *International Journal of Child-Computer Interaction*, 31:100446, 2022.

[6] Serge Egelman, Julia Bernd, Gerald Friedland, and Dan Garcia. The teaching privacy curriculum. In *ACM Technical Symposium on Computing Science Education*, pages 591–596, 2016.

[7] Chris Fennell and Rick Wash. Do stories help people adopt two-factor authentication. *Studies*, 1(2):3, 2019.

[8] Batya Friedman, David Hurley, Daniel C Howe, Helen Nissenbaum, and Edward Felten. Users' conceptions of risks and harms on the web: A comparative study. In *CHI Extended Abstracts in Conference on Human Factors in Computing Systems*, pages 614–615, 2002.

[9] Rebecca Jeong and Sonia Chiasson. 'Lime','open lock', and 'blocked': Children's perception of colors, symbols, and words in cybersecurity warnings. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[10] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. In *Symposium On Usable Privacy and Security*, pages 39–52, 2015.

[11] Albana Kona, Giacomo Martirano, and Guglielmina Mutani. The european commission's science and knowledge service. 2019.

[12] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children*, pages 67–79, 2018.

[13] Priya C Kumar, Fiona O'Connell, Lucy Li, Virginia L Byrne, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. Understanding research related to designing for children's privacy and security: A document analysis. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference*, pages 335–354, 2023.

[14] Sana Maqsood and Sonia Chiasson. Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):1–37, 2021.

[15] Sana Maqsood and Sonia Chiasson. "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2021.

[16] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies*, 2018(4):5–32, 2018.

[17] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security*, pages 1–18, 2022.

[18] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1–17, 2012.

[19] Fahimeh Raja, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov, and Kellogg S Booth. It's too complicated, so i turned it off! expectations, perceptions, and misconceptions of personal firewalls. In *ACM workshop on Assurable and usable security configuration*, pages 53–62, 2010.

[20] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. “woe is me:” examining older adults’ perceptions of privacy. In *CHI Extended Abstracts in Conference on Human Factors in Computing Systems*, pages 1–6, 2019.

[21] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they’re trying to tell me something: Advice sources and selection for digital security. In *IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[22] Sukamol Srikwan and Markus Jakobsson. Using cartoons to teach internet security. *Cryptologia*, 32(2):137–154, 2008.

[23] Miriam Sturdee, Lauren Thornton, Bhagya Wimalasiri, and Sameer Patil. A visual exploration of cybersecurity concepts. In *Creativity and Cognition*, pages 1–10, 2021.

[24] Sangho Suh, Sydney Lamorea, Edith Law, and Leah Zhang-Kennedy. Privacytoon: Concept-driven storytelling with creativity support for privacy concepts. In *Proceedings of the ACM Conference on Designing Interactive Systems*, pages 41–57, 2022.

[25] Rick Wash. Folk models of home computer security. In *Sixth Symposium on Usable Privacy and Security*, pages 1–16, 2010.

[26] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[27] Leah Zhang-Kennedy, Robert Biddle, and Sonia Chiasson. Secure comics: An interactive comic series for improving cybersecurity and privacy. In *International BCS Human Computer Interaction Conference*, pages 1–3, 2017.

[28] Leah Zhang-Kennedy and Sonia Chiasson. A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, 54(1):1–39, 2021.

[29] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. Stop clicking on “update later”: Persuading users they need up-to-date antivirus protection. In *International Conference on Persuasive Technology*, pages 302–322. Springer, 2014.

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