Co-Designing Online Privacy-Related Games and Stories with Children

Priya Kumar[1], Jessica Vitak[1], Marshini Chetty[2], Tamara L. Clegg[1], Jonathan Yang[2], Brenna McNally[1], Elizabeth Bonsignore[1]
College of Information Studies[1], University of Maryland, College Park, USA
Department of Computer Science[2], Princeton University, New Jersey, USA
{pkumar12, jvitak, tlclegg, bmcnally, ebonsign}@umd.edu {marshini, jjy}@princeton.edu

ABSTRACT
Children ages 8-12 spend nearly six hours per day with digital content, but they receive little formal instruction related to managing privacy online. In this study, we explore how games and storytelling can inform the development of resources to help children learn about privacy online. We present results from three co-design sessions with a university-based intergenerational design team that included eight children ages 8-11. During these sessions, we reviewed existing privacy resources with children and elicited design ideas for new resources. Our findings yield several recommendations for designers. Specifically, online privacy-focused educational resources should: (1) include relatable elements such as familiar characters and easily understandable storylines, (2) go beyond instructing children through "dos and don'ts" and equip children to make privacy-related decisions, and (3) expose children to a range of privacy consequences, highlighting the positive and negative outcomes that can result from disclosing and managing information online.

Author Keywords
Children; privacy online; mobile games; storytelling; narrative; Cooperative Inquiry; co-design.

ACM Classification Keywords
• Security and privacy ~ Social aspects of security and privacy • Social and professional topics ~ Children

INTRODUCTION
Children ages 8-12 spend nearly six hours per day engaging with various forms of digital content [12]. While the Children's Online Privacy Protection Act (COPPA) restricts what information operators of websites and online services in the U.S. can collect on children under the age of 13, many mobile apps fail to abide by the law's provisions [20,21]. As we know from analyses of digital trace data, personal information, likes, and preferences can be inferred from seemingly innocuous data sources, such as a list of movies one has watched on Netflix [4] or keywords entered into a search engine [3]. This means that from a young age, children may be unknowingly revealing information about themselves just by going online. In present times, children's online interactions are moving beyond websites and mobile devices to include Internet-connected toys, personal assistants like Amazon Echo, and other digital tools. Thus, the need for privacy-focused research and design regarding the youngest technology users is increasingly important.

Addressing this need, ACM's Child-Computer Interaction Special Interest Group now includes privacy as an area of focus [31,32]. Likewise, various organizations have developed resources to help teach children about privacy online [22,24]. While some have created curricular materials to teach children about privacy in school [25,44], most children do not receive formalized privacy education [28,41,46]. Boosting children's knowledge of privacy online can equip them to make more informed choices when interacting online and recognize how they can protect their personal information [35,47,58].

Working with children as co-designers can help researchers understand the best ways to design educational resources that facilitate learning about the complex and nuanced concepts related to privacy online [27]. Already, prior work has found that games and storytelling work well to teach children about topics related to science, technology, engineering, and mathematics (STEM) because they help children understand how real-world complexities shape decision making [2,23]. For instance, research teams have created an immersive game [47] and a comic book-based interactive story [58] to teach children about privacy online. We used a distinct co-design research method—Cooperative Inquiry (CI)—to study how different forms of gaming and storytelling—a simple mobile game and a Choose-Your-Own-Adventure (CYOA) story—can enhance children's learning about privacy online. Our primary focus in this study was not to develop and test a specific tool, but rather, to elaborate ideas about how to engage children effectively in learning about privacy online. To do so, we explored the research question: *How can co-designing games and interactive narratives with children inform the development of privacy-focused educational resources?*

Below, we present findings from three co-design sessions conducted in Fall 2017 with an intergenerational design team

IDC '18, June 19–22, 2018, Trondheim, Norway © 2018 Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-5152-2/18/06...$15.00
https://doi.org/10.1145/3202185.3202735

at the University of Maryland that included eight children ages 8-11. In the first session, we examined three types of existing resources: an online game, a narrative-based video series, and a text-based quiz app. In the second session, we iterated on a low-fidelity prototype of a privacy-related game whose design was informed by our takeaways from the first session. In the third session, child partners created interactive privacy-based narratives in the form of CYOA stories, an activity that also grew out of themes we identified in the first session. Based on our findings, we offer recommendations for designing privacy-related educational resources for children.

RELATED WORK

In this section, we explain the importance of privacy for children, review existing empirical and design work exploring children's conceptualizations of privacy online, and discuss how games and storytelling inform children's learning. We then describe the CI method of participatory design used in this study.

Why Privacy is Important for Children

Privacy is a complex concept that eludes simple definition. In the context of social interaction, privacy involves disclosing information (or deciding not to), as well as managing boundaries between different contexts in one's life [43]. When such disclosure occurs online, privacy is less about control and more about the appropriate flow of information [42]. Even though children are under the care of parents or guardians, they still need privacy [52]. Privacy gives children space to practice making decisions, to create boundaries, and to experience the outcomes, both positive and negative, of their decisions [43]. Children interpret privacy online as "unintended others watch[ing] them," and they do not equate disclosing information online with relinquishing privacy [51, p. 6]. Having privacy online helps children experiment with different types of behavior or identities, communicate with others, and build relationships [37]. As the everyday lives of children increasingly involve online interactions, it is important to help them understand how to protect their privacy online.

Children's Conceptualizations of Privacy Online

A few studies have worked directly with children to explore their conceptualizations of privacy online. For example, one study found that children ages 5-11 largely understood that certain types of information (e.g., address, password) were sensitive and that information could be appropriately shared with some actors (e.g., parents, teachers) but not others (e.g., unknown people) [35]. However, children under age 10 largely did not recognize that managing privacy online involves additional considerations (e.g., adjusting privacy settings, minimizing the spread of sensitive information by only disclosing it face-to-face). Another study found that children ages 7-11 perceived privacy threats to come primarily from peers and "bad" media, in the form of others touching or viewing devices while children used them, others accessing and changing children's information, and children viewing content that contained violence or inappropriate language [59]. With regard to Internet-connected toys, one study found that while children ages 6-10 understood that the toys could "remember" what children say via recording, they largely did not appear to connect the ability to record with the ability for others to *hear* the recordings [39].

These studies shed light on how children view privacy in relation to Internet-connected technologies, and the findings highlight areas where educational resources can enhance children's understanding of privacy online. While government agencies [22], nonprofit organizations [24], and educational institutions [44] have produced resources meant to teach children about these topics, little research has studied their effectiveness. Furthermore, it is often unclear whether or to what extent children participated in the development of those resources or whether children find existing resources engaging and helpful for exploring and learning about privacy online.

Notably, researchers from two projects have worked with children to develop resources that teach aspects of privacy online. These resources include a hybrid board/computer game called "The Watchers," which helps players learn how websites collect information and use it for marketing [47], and an interactive, electronic comic book called "Cyberheroes" that uses a superhero motif and multimedia elements to teach children lessons related to "personal information, online chatting, location sharing, cyberbullying, and passwords" [58, p. 11]. These studies used a particular modality—an experiential game or interactive comic book—and methodology—participatory action research or user study— respectively, to create new resources for teaching children about privacy online. We extend this work by using the Cooperative Inquiry (CI) method to evaluate and co-design game- and story-based resources with children to better understand the design space for teaching children about privacy online.

Helping Children Learn through Games and Storytelling

Our focus on game- and story-based resources for learning about privacy online builds on prior work in the learning sciences that highlights the unique affordances of these modalities for supporting learning. Games have been used to engage learners in a range of topics, including history, geography, math, and health [5,6,23,54]. Likewise, digital storytelling has been used to promote literacy, history learning, and content instruction in STEM as well as health education contexts [7,8,10,48].

Both approaches immerse learners in narratives, leveraging key elements of stories (e.g., climax, pacing, character perspective) to naturally engage children in content- and process-oriented practices [53,54]. For example, Barab et al.'s [2] Quest Atlantis game environment positions late elementary-aged learners as aliens in a series of virtual worlds who carry out quests aligned with various academic subjects (e.g., statistics, persuasive writing) Similarly, Clegg et al. [11] leveraged a digital storytelling app called StoryKit to help children learn and engage in science inquiry through

telling stories about their life-relevant science investigations. They found that the elements of telling a story (e.g., describing the setting and purpose of the story, sequencing the narrative) scaffolded the process of inquiry for learners as they created stories with pictures, audio, drawing, and text on the app. While narrative has been used to support learning in a variety of technology systems and designs beyond games and digital storytelling applications (e.g., video narration, social media tools, virtual worlds), few studies have explored its applicability for privacy learning [*cf.* 47,58]. In this study, we explore how children might want to design narrative-based systems to support privacy learning through games and storytelling.

The Cooperative Inquiry Method

In the technology development process, children can take on various roles—users, testers, informants, and full design partners [17]. The first two roles focus primarily on obtaining feedback or input from children at the end of the design cycle. The latter two roles focus on idea elaboration, where adults and children share ideas and build on them together [26]. CI places children in various roles throughout the entire iterative design process [17].

CI is a participatory design method where adults and children work as design partners to create technologies with and for children [16,26]. CI typically involves a team of 6-8 children and several adults who meet regularly [26]. The method focuses on children ages 7-11 because they understand the abstract idea of informing future technologies and can discuss their thoughts, but they are not constrained by ideas of how things "should" work [16]. CI sessions shift focus away from the typical power structure in which adults exercise authority over children, instead emphasizing partnership between children and adults. For example, sessions often begin with a snack and casual conversation; participants wear informal clothing; and children do not need to raise their hands to speak nor refer to adults by their titles or last name (e.g., Ms. Lee) [17,26].

Child (pseudonym)	**Age** (years)	**Sex**	**Session 1**	**Session 2**	**Session 3**
Addie	8	F	✓	✓	✓
Ben	8	M	x	✓	x
Cory	8	M	✓	✓	✓
Henry	10	M	✓	✓	✓
Drea	11	F	✓	✓	✓
Emily	11	F	✓	✓	x
Fiona	11	F	✓	✓	✓
Gervais	11	M	✓	✓	✓
Adults #	-	-	7	9	9

Table 1. Participants who attended co-design sessions.

METHOD

To examine our research question, we held three CI sessions with Kidsteam, a University of Maryland-based intergenerational design team, in November and December of 2017. The team, which includes several adult researchers and eight children ages 8-11, meets for 90-minute co-design sessions twice a week after school throughout the academic year, and generally full-time for two weeks in the summer.

All eight children on the team attended at least one of our sessions, and six attended all three. Table 1 provides basic demographic information about the children on the team, indicates which sessions they participated in, and lists how many adult partners joined each session. All names are pseudonyms. Adult partners included the design team's facilitators and this paper's authors.

Each 90-minute session followed a typical CI format [17,26]. After eating a snack together, the adult and child partners sat in a circle and each answered the "Question of the Day." This was an open-ended question related to that session's topic (e.g., What is an example of something that is private and why?). An adult partner then explained the session design prompt and activity. Participants broke into small groups of 2-3 children and a few adults and completed the design activity. Afterward, each group presented its work to the whole design team and an adult partner recorded each group's ideas on a whiteboard. The adult partners quickly summarized emergent themes across groups and gave child partners a chance to ask questions and make adjustments. After the session ended and the children left, the adult partners discussed insights from the session. Table 2 briefly summarizes each session's activity.

Data Analysis

Each session yielded a variety of data, including design ideas that the team drew and wrote during design activities, notes from group presentations at the end of each session, and notes from discussions about emerging themes. To analyze the data, we reviewed artifacts from the design activities

Design Session	**Summary of Design Activity**
Session 1	Child partners reviewed existing resources (an app, a game, and a video series) related to privacy online and offered suggestions to improve them.
Session 2	Child partners annotated a low-fidelity prototype of a modified version of the mobile game Doodle Jump [14]. The prototype incorporated privacy-related elements based in part on findings from session 1.
Session 3	Child partners used Marvel's Prototyping on Paper (POP) application [45] to create their own narratives that incorporated questions related to privacy online. The activity was based in part on findings from session 1.

Table 2. Overview of the activities completed at each co-design session.

Figure 1. Resources children reviewed during the first session. Mindful Mountain [40], a privacy-related interactive online game (left, image © Google), King GAFA [33], a narrative-based video series about online privacy (center, image © Pichlbauer et al.), and TechSafe Privacy [18], a mobile application for teaching privacy online (right, image © Excite-ed).

(e.g., sheets of paper on which the team drew ideas), photographs of notes from the whiteboard, and hand-written notes. Three authors synthesized the key themes into session reports and the full author team analyzed these session reports, discussing and refining the main themes until it achieved consensus on the final set of findings [19]. The following section describes each session's design activity and findings.

DESIGN ACTIVITIES AND FINDINGS

Design Session 1: Reviewing Existing Privacy Resources

The goal of the first session was to review existing resources related to privacy online. First, we compiled a list of publicly available, privacy-focused resources, based on input from experts as well as searching online. We selected three resources that reflected different types of interaction (game, video, mobile app), developers (multinational company, university students, small educational technology company), and topics (sharing too much information online, data mining, handling personal information). Figure 1 depicts each resource, which we describe in greater detail below.

Interactive Online Game

The online game Mindful Mountain [40] is part of Google's Be Internet Awesome program, which launched in June 2017 [13].[1] Players become characters ("Internauts") in the fictional world of Interland. The Internaut bounces beams of light off mirrors to hit certain figures and avoid others. Each beam of light represents a "post" the character is supposed to "share" only with specific people (e.g., family, friend). We selected this game because its focus on inappropriate disclosure of information online clearly relates to privacy. Other games in the program focus on security, information credibility, and civility online. Google partnered with nonprofit organizations such as the Family Online Safety Institute and ConnectSafely to develop the program, though it is unclear whether the company incorporated feedback from children when designing or evaluating the game.

Limited-interaction, Narrative-based Videos

King GAFA [33] is a series of short videos created by design students at Vienna's University for Applied Arts and released in 2017. It uses a fairy tale motif to explain how the data collection practices of major Internet companies threaten users' privacy. King GAFA (a personification of Google, Apple, Facebook, and Amazon) gives peasants tools to harvest the magical binary crop of ones and zeros, and they happily give their crop to him. This allegory is meant to represent how people—through their use of digital devices and services—generate valuable data (and profit) for major Internet companies. The video's designers consulted privacy experts when creating the story, but it does not appear they sought input from children. The videos are not explicitly meant for children, but the incorporation of fairy tale elements encourages their use for younger audiences.

Text-based Quiz App

The TechSafe Privacy mobile application [18] is part of a group of mobile apps developed by Excited-ed, a U.K.-based educational technology company, in partnership with various schools in England. The app, which is available on Apple's App Store and Google's Play Store, includes tips related to online reputation, privacy, and identity theft. Users swipe through screens that define each concept and offer general guidelines (e.g., "Never reveal your personal details when talking to people in chatrooms or game sites"). A 10-question multiple-choice quiz reviews concepts discussed in the app.

Design Activity

Seven children and seven adults participated in Session 1. The room had three stations, one for each resource, and an adult partner staffed each station. The design team broke into three groups (each with 2-3 children and one adult) and rotated through the stations. An adult partner explained the resource, and child partners spent 12 minutes interacting with and discussing each resource. The team used the sticky noting evaluation technique [19,26,56,57], where partners wrote their likes, dislikes, and design ideas on Post-it notes and clustered them on a large sheet of paper. While adult

[1] This study was funded in part through a Google Faculty Research Award. No one from Google was involved in the research. The team selected this game because it was relevant and fairly new.

partners sometimes asked child partners questions (e.g., "How would you change that") and wrote down children's comments, they largely refrained from sharing their own opinions. Child partners also received paper journals in which they answered three Likert-scale questions for each resource (scale: -2 = Strongly Disagree through 2 = Strongly Agree, with 0 = Neutral):

- I enjoyed this activity.
- This game helps children learn about online privacy.
- This activity would help kids talk to their parents about online privacy.

At the end of the session, the adult partner from each station summarized the likes, dislikes, and design ideas, which the child and adult design partners discussed as a group [19,26,56].

Findings from Design Session 1

Based on their responses to the Likert-scale questions in Session 1, the seven child partners most enjoyed the interactive online game (M=1.43, SD=0.98) and least enjoyed the text-based quiz app (M=-0.29, SD=1.25). They found the quiz app most educational (M=1.29, SD=0.95) and the narrative-based videos least educational (M=-1.29, SD=0.76). They said the quiz app was most useful in helping children talk about online privacy with their parents (M=0.71, SD=0.76) and the videos were least useful in this respect (M=-1.14, SD=0.90).

Below, we discuss the three primary takeaways that emerged from the child partners' likes, dislikes, and design ideas.

Incorporate Design Features that Help Children Understand the Purpose of the Privacy-Related Resource

Echoing prior work, children in this session enjoyed interactive media [49]. Child design partners found the online game "*fun*," and they liked its colors, lights, and graphics. For the videos, children liked their pictures, animation, and music. For the quiz app, child partners liked its colors, but the sticky notes suggest they did not find it exciting: "*It's boring, not much fun.*"

Child partners wanted features that would help them understand each resource. Design ideas suggested the game include more instructions and hints. The online game gave instructions before each round, but the children often clicked right through without noticing this text. For the videos, several clusters of dislikes emphasized confusion. One dislike note read, "*What, not making sense,*" another, "*Don't know what they're talking about.*" Conversely, the quiz app's familiar interaction mode—guidelines and a quiz—meant that the children quickly recognized how they were supposed to use it. One sticky note said it was "*Easy.*"

Craft Narratives that Clearly Connect to Privacy

The two narrative-based resources take place in fictitious worlds—the game in "Interland" and the videos in an unidentified kingdom. A theme that consistently emerged across the children's dislikes for both resources was that they lacked a clear connection to privacy. While discussing the videos, some child partners said a fairy tale motif could be useful to teach younger children about privacy, but it would need to more clearly link the story to the concepts. One design idea said a prince or princess could lock away their information only to have the key stolen by a monster or pirate. Another suggested a story where a king makes privacy rules. A third design idea suggested the videos could incorporate more positive feelings rather than focus solely on threats to privacy.

Another cluster of dislikes suggested that some children found it confusing to see "new" technology appear in an "old" world. One design idea suggested that the story "*shift timeframe to future, since they added future tech.*" 11-year-old Fiona asked, "*How is this going to teach me about real world privacy if I don't hear real world stories about how people lost their privacy?*" This echoed a theme that emerged in the discussion of all three types of resources. Child partners wanted more authentic stories that included "*real life examples*" and outcomes to help children understand why they should pay attention to privacy.

Give Children Clear Takeaways Related to Privacy

While child partners deemed the quiz app least enjoyable, they also said it was the most educational and most likely to spark conversations about privacy. 11-year-old Emily said the other resources "*didn't really talk about privacy, so you wouldn't have anything to talk with your parents about if you didn't know what it was or what not to share and stuff, while [the app] did.*" Children identified specific facts they learned from the app, such as the definition of phishing. Two like notes explicitly supported the quiz. A cluster of design ideas offered ways to improve its range of interactivity, such as adding more questions and levels of difficulty.

Design Session 2: A Privacy-Focused Mobile Game

The results from the first design session suggested that, while child partners found the interactive game most entertaining out of the three resources, its lack of a clear connection to privacy limited its utility as a learning tool.

Using this feedback, we developed a low-fidelity prototype in Microsoft PowerPoint of a game based on Doodle Jump [14], a popular platforming game/app. In it, players navigate a character (the Doodler) up a scrolling screen by jumping from one platform to another. Our prototype, while low-fidelity, was a working model that permitted prescribed interactions to give children the functional "look-and-feel" [30] of how a potential game could be played.

Our goal with this prototype, which we called "Privacy Doodle Jump," was to elicit ideas about how to engage children in learning about privacy. Since children in session 1 sought clear privacy-related takeaways and enjoyed the mobile app's quiz, we added scenario-based, multiple-choice questions to Privacy Doodle Jump (See Figure 2). By scenario-based, we mean that the questions described a situation and asked how the person in the situation should

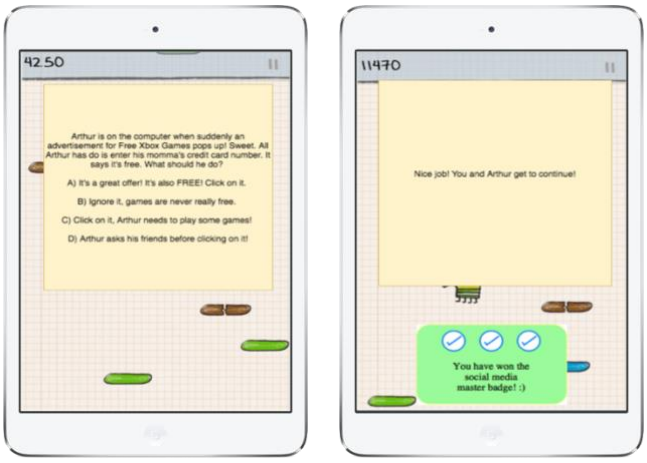

Figure 2. Screenshots from the Privacy Doodle Jump [14] mobile game prototype used in design session 2. Image modified, © Lima Sky.

respond, rather than framing quiz questions as truisms. For example, one question asked how a character would respond to an advertisement that popped up online and asked for a credit card number. If the player selected the correct answer, an encouraging message and explanation appeared on the screen. If they selected an incorrect message, the prototype displayed the correct answer along with an explanation. The questions related to a particular theme; after answering at least three questions in a row correctly, players would earn a badge. Figure 2 shows a player winning the "Social Media Master" badge.

Questions appeared when Doodlers were about to receive special "power-ups"—such as a helicopter hat to move ahead quickly. Questions also appeared when Doodlers fell off platforms. In the real Doodle Jump, the game ends immediately after the Doodler falls. In Privacy Doodle Jump, players who answered a question correctly after falling earned a second chance to continue playing.

Eight children and nine adults participated in session 2. Each child partner spent five minutes playing the original Doodle Jump on an iPad or iPod Touch to get a sense of how the game worked (though nearly all were familiar with the game). An adult partner then walked the children through the Privacy Doodle Jump prototype. The design team broke into three groups, each with 2-3 children and three adults. Each group received a packet of printouts of the prototype screens, scissors, markers, and tape. We used the "Big Paper" paper-prototyping technique [56], where design partners directly iterate upon previous designs by cutting out and marking up printouts with their suggestions, additions, and changes. This technique emphasizes idea elaboration [26], in which child and adult design partners build on ideas together. After working on this task for 30 minutes, the groups came together and each group presented their ideas while an adult partner took notes. The adult partners synthesized Big Ideas across groups and refined these ideas based on a discussion with the children [19,26,56].

Findings from Design Session 2

Educational games must promote learning goals while also engaging players. Children are sensitive to this balance; after we introduced Privacy Doodle Jump, 11-year-old Gervais, muttered under his breath, "*I hate it when they take a perfectly good game and they try to make it educational.*" Child partners came up with various ideas to better embed privacy-related educational components into gameplay. Below, we summarize the three main takeaways that emerged from the Big Ideas.

Offer Incentives that Attract Children to Keep Playing

Child partners wanted features that allowed players to customize aspects of the game, which could entice children to keep playing and learning about privacy online. For example, Cory suggested a "store" where players could select new avatars or buy power-ups. Fiona thought a store should have seasonal outfits and other ways to customize the Doodler's appearance. They suggested that players could gain access to these elements as rewards for high performance in the game. These recommendations echo features seen in other popular mobile apps. For example, Pokémon Go players can change their avatar's outfit or purchase space to collect more Pokémon [9].

Child partners had similar recommendations to improve how badges functioned in the game. All child partners agreed that badges, by themselves, lacked appeal. A few suggested calling them "achievements" instead. Connecting badges to other rewards (e.g., in-game power-ups, items to customize the avatar) could also motivate players to engage with the privacy features of the game. For example, Henry suggested that obtaining a privacy achievement badge could unlock a new type of power-up to use in the game.

Integrate Privacy Education Seamlessly into Gameplay

One of the greatest challenges in developing educational games is the need to balance fun with learning [34,36]. Child partners agreed the prototype veered too far into the educational space to be appealing to a general audience, and they provided several design recommendations to better embed the privacy education components—particularly the quiz-style questions—into gameplay to make it less disjointed. Emily suggested the creation of "*question zones*," where the player moves the avatar over the correct answer (See Figure 3). This integrates questions into gameplay rather that than interrupting it [23]. Alternatively, if the game kept the original format where questions pop up and stop gameplay, Drea and Cory suggested shortening the question length, reducing the number of response options, and offering audio or video capabilities. Their suggestions would reduce the reading involved in gameplay and curtail interruptions to play mechanics and game flow while retaining the privacy-related content. Children also agreed that a player who gets a question correct should get an immediate boost (e.g., temporary invincibility, higher jumping ability).

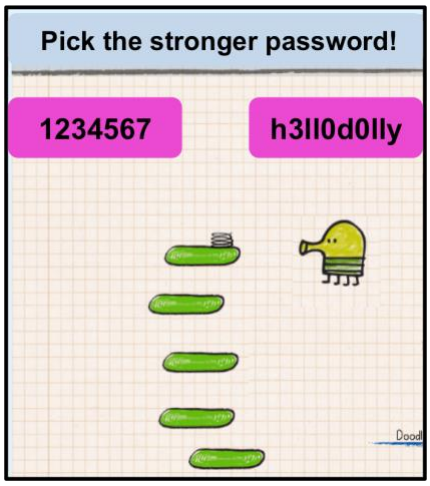

Figure 3. An iteration of a screenshot from the Privacy Doodle Jump [14] prototype that shows an example of a "Question Zone" Image modified, © Lima Sky.

Expand Privacy Components Beyond Questions to Reinforce Educational Lessons

In our prototype, the only significant change to Doodle Jump's original gameplay was the addition of the pop-up privacy-related questions. Our child partners suggested several ways beyond questions to integrate privacy into gameplay. These included creating themed boards (e.g., have the background look like the inside of a computer with wires and chips), labeling platforms with privacy-related information, and including privacy-themed monsters (e.g., viruses, bullies) and power-ups.

All design groups envisioned changing the game format from continuous scrolling (i.e., the player continues upward until they die) to a set of self-contained boards. This would facilitate a number of other recommended features, such as themed boards, distinct levels, and a connection between badges and tangible outcomes (i.e., completing a level). Having discrete boards could also provide greater context for the embedded *question zones*. To reinforce the game's educational focus, a pop-up message at the start of each board could present that board's general theme. For example, the question in Figure 3 could be part the "account security" board, and the background image could show a computer login screen. Monsters and power-ups linked to the board's theme could also highlight the educational message. For example, Henry suggested a monster labeled "hacker" could float in the account security board, signifying someone who wanted to steal a password, and a power-up labeled "strong password generator" could boost the player through the board. This would build on a feature of the actual Doodle Jump game, which includes themed versions for holidays [15,29].

Design Session 3: Privacy-Focused Interactive Stories

Results from the first design session suggested that while children found the idea of privacy-related narratives compelling, the storylines in existing materials such as the King GAFA videos produced more confusion than learning. To get a sense of what types of storylines would resonate with children when discussing privacy online, we invited children to create a Choose-Your-Own-Adventure (CYOA) story using an interactive mobile application.

In CYOA stories, the reader makes choices that determine the main character's actions and lead to different outcomes [1]. Where a traditional narrative contains a fixed storyline, CYOA stories invite the reader to actively construct the storyline. We wanted to understand the types of storylines and story elements (e.g., characters, topics, plots, climaxes) that children would create related to privacy online. Additionally, we wanted to analyze their stories to get a sense of their understanding of privacy issues and how they envisioned addressing them.

Six children and nine adults participated in session 3. Each child partner worked with adult researchers to create a CYOA story using Marvel's POP (Prototyping on Paper) app [45], which child partners learned to use during a previous session. The POP app facilitates the creation of interactive prototypes by allowing users to import photos of paper-based drawings or mock-ups, make certain portions of the images "active" (e.g., draw buttons), and link the images. The app then allows a user to navigate through the prototype, moving through the screens to simulate the prototype's use and functionality. Hence, this session used a modified, digitized version of the paper prototyping technique [56].

At the session, one adult partner briefly introduced the design team to the concept of a CYOA story. The design team then divided into three groups, each with two children and three adults. Each child received paper, markers, and an iPad loaded with the POP app. We asked each child partner to come up with their own CYOA story about how children do things online. We told them to envision that these stories would be used to teach other children about privacy online. Child partners could include as many decision points as they wanted, but we asked them to include the following two questions related to privacy online:

- Would you like to switch on your location settings so it's possible to know where you are? (Yes or No)
- Would you like to store your password so you don't have to type it in the future? (Yes or No)

We selected these prompts because they referenced types of information that would be familiar to children–passwords and location–and because they raise different types of privacy concerns based on contextual factors. For example, sharing location with parents may be more appropriate than sharing it with all users on a given app, and storing a password on one's own device may be more appropriate than storing it on a public computer.

Child (Age)	Premise	Decision Points	Outcomes
Addie (8)	Friends Serena, Molly, and Derek meet at the mall.	• Whether Serena checks in at a donut shop • Whether Molly gives a smartphone access to various types of personal information • Whether Serena and Molly respond to a text from an unknown person • Whether Serena gives the unknown person (later revealed to be a 25-year-old man) her address (so he can share a box of donuts with her)	None specified
Cory (8)	A boy named Timmy receives a smartphone for Christmas.	• Whether Timmy saves a password on the new phone	Someone steals the password, breaks into Timmy's house, steals the remaining presents, logs into the phone, and sends mean messages to Timmy's friends.
Henry (10)	The reader receives a suspicious email purportedly from a former classmate	• Whether to click a link in the email or tell your parents about the email • Whether to give the website access to your location • Whether to save your password on the website	If the reader goes to the website and says yes to the other questions, the story says, "The end. You got hacked."
Drea (11)	A girl named Sara receives a text from an unknown number.	• Whether Sara responds to the text or blocks the number. • Whether Sara turns location to let the texter (who is her crush) come over and bring flowers • Whether Sara shares her phone's password with her father, so he can block the number.	If the girl reveals her location, the crush murders her mother. The girl has the option to run to her father for help.
Fiona (11)	The reader finds a smartphone on the ground.	• Whether to pick a lost smartphone off the ground • Whether the phone has a password • Whether to go to the house of the phone's owner	None specified
Gervais (11)	Professional football player Odell Beckham Jr. sets up social media accounts.	• Whether Beckham Jr. shares his location while setting up an Instagram account	If Beckham Jr. shares his location, a rival player breaks into his house and steals his valuables.

Table 3. Summary of the CYOA stories that child partners created during Session 3.

Child partners drew mock-ups of scenes from their stories, took pictures of each scene, and used the POP app to link them together. While child partners initiated and crafted the overall storylines and character conflicts for their stories, the adult partners built upon the children's ideas by answering questions, offering suggestions, and helping input their paper-based designs into the POP app. After 35 minutes, each child presented their story while an adult took notes. The adult partners identified Big Ideas observed across stories and refined them based on a discussion with child partners [19,26,56].

Findings from Design Session 3

Table 3 includes summaries of the child partners' CYOA stories, indicating where readers could make choices for the main character. Below, we describe one story in-depth and discuss three takeaways that emerged across the six stories.

Gervais, 11-year-old boy: No Title

Gervais' story focused on an American football team. The main character was Odell Beckham Jr., a famous professional football player. In the story, Odell and his teammates were at practice when Odell made a nice one-handed catch. His teammates wanted to post his catch on Instagram but Odell said, "Wait! I don't have an account." Odell's teammate Eli Manning, another famous player, already had an account. Eli exclaimed, "Hey! Odell! Let's set you up with an account! My score is 4000 already—do you want your location set up?" The next screen depicted an app store that showed the different social media sites they decided to set up. The story asked if Odell would share his location with the app (options: yes or no). Eli stated that other teammates used location sharing to meet up. If the reader selected no, Odell would not be able to go to the maps and see his friends and teammates. In that case, Eli would state, "Man, that's okay, we'll just text you where we are." If the reader selected yes, then Jay Cutler (a famous player on a rival team) would see Odell's location, go to his house after Odell left, and steal Odell's valuables. The story would end with Odell crying when he found out.

Incorporate Elements Related to Everyday Life, Even in Fictional Stories

All stories were fictional, but some focused on figures from popular culture (e.g., Odell Beckham Jr. and Eli Manning in Gervais' story) while others had more "everyday" characters

(e.g., young Timmy in Cory's story). The stories also incorporated elements of everyday life. Drea's story included a "crush" and Henry's story re-created Google's interface. This highlights the importance of including elements in resources that are relatable to children.

Help Children Recognize Routine, Rather than Drastic, Consequences of Privacy Decision Making

When characters chose options that generally protect privacy (e.g., not saving passwords, not sharing location), the story typically ended. Conversely, when characters did not choose privacy-protective options, the story often led to a drastic end, including murder and burglary. In addition, two of the stories lacked clear outcomes. This suggests that children are used to thinking about privacy as a black-and-white issue, where the consequences are unclear or dire. It highlights an opportunity for resources that help children recognize the nuances in privacy decision-making.

Encourage Children to Reflect on the Complexity of Privacy Decision Making

In some cases, child partners did not initially recognize the complexity of the privacy decisions they included in their stories. Some wondered why anyone would choose the least privacy-protective option. For example, 11-year-old Gervais wondered why anyone would share their location. Adult partners explained that sometimes sharing location might be convenient or useful. One adult gave the example of an app she uses that controls the physical locks on her doors. She explained that sharing her location allowed the app to unlock her door when she was at her house without using her keys. Gervais then talked about how social media apps like Snapchat can show users where all of their friends are if given access to the user's location. He then decided to add that to his story. This suggests the value in creating resources that encourage children to reflect on situations that involve privacy-related decisions, rather than simply offering the "do's and don'ts" of privacy online.

DISCUSSION

All three co-design sessions emphasized that, when presented with educational resources related to privacy online, children want to understand their purpose, how to use them, and what takeaways they offer for everyday life. Materials designed to teach children about privacy online often focus on do's and don'ts. Such straightforward guidelines can be useful when introducing children to complex subjects like privacy, or when working with younger children. Yet relying too much on this format risks oversimplifying what privacy—a complex, contextual, and nuanced subject [42]—means when managed online. Furthermore, this does little to equip children to learn how to make decisions related to privacy online. Such skills are important as children grow and gain greater autonomy to make decisions about what information to disclose online [43]. Below, we offer recommendations for designers and others who seek to create educational resources to teach children about privacy online.

Recommendations for Designing Engaging Resources To Teach Children About Privacy Online

Use Privacy Scenarios Related to Children's Everyday Lives

Across all design sessions, children best understood privacy-related takeaways when the resources contained elements that reminded them of their everyday lives. This makes sense given that children already engage in a variety of online activities [12] and have opinions about the importance of privacy online [51].

We suggest that privacy-focused resources for children incorporate relatable elements such as familiar characters (e.g., other children, famous athletes), recognizable online services (e.g., Instagram), and easily understandable storylines (e.g., how to set up a new smartphone). For example, Harvard's Berkman Klein Center partnered with the public broadcaster PBS Kids to create a media literacy curriculum using the popular character Ruff Ruffman [50]. Privacy resources can also invite children to customize certain components, such as character names or types of online platforms discussed. Using familiar elements and inviting children to interact with a resource can make children feel more invested in the material and thus more receptive to its messages.

Equip Children to Learn Privacy Decision-Making Skills

Our design sessions suggest that existing resources may focus too much on privacy-related information and not enough on developing the skills to navigate privacy online. We recommend that resources for teaching children about privacy online go beyond telling children "do's and don'ts" and incorporate features that help children learn how to make privacy-related decisions. Analogies to the physical world can help, but it is important to highlight how seemingly similar situations actually differ [42]. For example, children are often told not to speak to strangers. In the physical world, children can easily determine through sight and sound whether someone is a stranger, and they can use contextual cues (e.g., surroundings, parental reaction) to figure out how to respond. A child probably feels more comfortable talking to a server in a restaurant than a passerby on the sidewalk because contextual cues and norms suggest the former is a more appropriate situation in which to engage with a stranger. Determining whether to respond to a message from someone online requires evaluating different contextual cues (e.g., app, username, language in the message). Educational resources should help children learn how to evaluate these contextual cues rather than offering one-size-fits-all advice.

Since children understand some of the contextual factors that influence privacy online [35], interactive resources can help them take their knowledge to the next level and discover what to consider when making a privacy-related decision. For example, instead of telling children not to share location information, resources can explain what someone should consider when an app asks for location information, such as who the location will be shared with and for what purpose. Our findings also offer empirical evidence for the need to

create engaging interactive experiences that promote these dialogues and reflection between children and parents or other trusted adults and peers. Resources can help prompt such conversations. An interactive app could send an email or text notification to parents about a child's progress on privacy-related lessons (provided the child is aware that parents receive these notifications), and a parent could follow up with the child about the lesson. Children could also receive artifacts, such as a certificate or a digital "achievements," to show their parents, which could prompt conversations.

Expose Children to A Range of Privacy Lessons with Positive and Negative Consequences

Our findings echo prior work that found children believe that revealing sensitive information online can result in such dire outcomes as burglary or kidnapping [35]. We suspect that this may be influenced by the way that children are taught about safety in general in school and at home—that not abiding by safety rules results in extreme consequences. We suggest that resources should explain positive as well as negative consequences of privacy-related decisions. For example, a child might want to enable location on an app like "Find my iPhone" so their parents can see where they are. Conversely, a child might want to disable location for a gaming app, since that information in unrelated to gameplay.

Prior co-design work found that children understand these types of privacy-related tradeoffs [38], which suggests that an opportunity exists to help scaffold children's learning in this area. In particular, resources can further push children to explore "grey" areas where the answer to a privacy-related decision is not black or white. Such materials can focus on helping children ask the right evaluative questions when making a privacy-related decision or help them develop a "privacy strategy toolbox" for deciding what to do [35]. For instance, when an app asks for location information, a child could ask, "Does this app need to know where I am?" When someone asks a child to provide information online, a strategy toolbox could suggest that a child "Ask a parent" or "Do not reply."

Privacy-related resources should also help children recognize that a range of consequences can stem from privacy-related decisions, rather than emphasizing the most drastic. For example, sharing location information with a large group of unknown people online can result in burglary, but it can also result in discomfort that a lot of unknown people know a private fact about you. Framing privacy-related decision-making this way focuses on the inherent value of maintaining privacy rather than privacy protection as a way to minimize harms.

Limitations and Future Work

Our study involved a set of eight children in three, 90-minute design sessions and evaluated only a subset of educational materials for teaching children about privacy online. Future work should build on these exploratory design recommendations to create fully functioning prototypes that can be evaluated with children through field deployments. Future work should also consider how such materials could be integrated into home and school contexts, something our research team is addressing. We have interviewed parents and children about privacy and security online [35] and are conducting focus groups with educators to understand whether and to what extent they incorporate lessons related to privacy and security online. We are also organizing a workshop focused on participatory design with children at the 2018 Symposium on Usable Privacy and Security (SOUPS) [55].

CONCLUSION

Now that children use smartphones and tablets to watch movies, complete homework assignments, interact with friends, and play games, it is more important than ever for children to begin learning about privacy online from an early age. Yet privacy education is rarely a formalized part of school curricula, especially during elementary and middle school [28,41,46].

With this study, we hope to inspire more work in this area. Through three Cooperative Inquiry sessions with an intergenerational design team, we explored how games and storytelling can inform the development of privacy-focused educational resources for children. We found that relevant, engaging narratives and games can be a powerful tool to help children more critically consider how to navigate privacy online. We recommend that designers who seek to create such resources go beyond instructing children through "do's and don'ts," equip children to make privacy-related decisions, and expose children to a range of privacy lessons, highlighting the positive as well as negative consequences that can result from disclosing and managing information online. Materials that incorporate these recommendations can help children practice asking privacy-related questions and making privacy-related decisions. Such skills will serve children well as they gain autonomy over decisions related to sharing information online.

ACKNOWLEDGMENTS

We thank all of the Kidsteam design partners for their enthusiastic participation. We also thank the anonymous reviewers for their feedback, which strengthened the paper. This research was supported by a Google Faculty Research Award. No one from Google was involved in the research.

SELECTION AND PARTICIPATION OF CHILDREN

This study's eight child participants, ages 8-11, are part of a university-based intergenerational design team. The team's child participants are selected from the team's wait list, which is open to new prospective child members. The team selects child participants at the beginning of each academic year, with the goal of balancing different ages and genders. The design team obtains parental consent and child assent at the start of each academic year. The design team is affiliated with the same HCI laboratory as five of this paper's authors. The university's Institutional Review Board approved the team's design activities.

REFERENCES

1. Angelia, S. et al. 2015. Design and evaluation of educational kinesthetic game to encourage collaboration for kindergarten children. *Proceedings of the 12th International Conference on Advances in Computer Entertainment Technology* (*ACE'15*). ACM Press, New York, NY, 1–5. DOI:https://doi.org/10.1145/2832932.2832967
2. Barab, S. et al. 2005. Making learning fun: Quest Atlantis, a game without guns. *Educational Technology Research and Development*. 53, 1 (Mar. 2005), 86–107. DOI:https://doi.org/10.1007/BF02504859.
3. Barbaro, M. and Zeller Jr., T. 2006. A face is exposed for AOL searcher no. 4417749. *The New York Times*.
4. Bennett, J. and Lanning, S. 2007. The Netflix Prize. *Proceedings of KDD Cup and Workshop 2007* (*KDD'07*), 3–6.
5. Bonsignore, E. et al. 2012. Alternate Reality Games as Platforms for Practicing 21st-Century Literacies. *International Journal of Learning and Media*. 4, 1 (Jan. 2012), 25–54. DOI:https://doi.org/10.1162/IJLM_a_00086.
6. Bonsignore, E. et al. 2013. Playing for real: designing alternate reality games for teenagers in learning contexts. In *Proceedings of the 12th International Conference on Interaction Design and Children (IDC '13)*. ACM Press, New York, NY, USA, 237–246. DOI=https://dx.doi.org/10.1145/2485760.2485788
7. Bonsignore, E. et al. 2013. Sharing Stories "in the Wild": A Mobile Storytelling Case Study Using StoryKit. *ACM Transactions on Computer-Human Interaction*. 20, 3 (Jul. 2013), 1–38. DOI:https://doi.org/10.1145/2491500.2491506
8. Bonsignore, E. et al. 2016. Traversing Transmedia Together: Co-designing an Educational Alternate Reality Game For Teens, With Teens. In *Proceedings of the 15th International Conference on Interaction Design and Children (IDC '16)*. ACM Press, New York, NY, USA, 11–24. DOI: https://doi.org/10.1145/2930674.2930712
9. Bradford, A. 2016. You can now customize your avatar in Pokemon Go, here's how. *CNET*.
10. Clegg, T. et al. 2014. Capturing Personal and Social Science: Technology for Integrating the Building Blocks of Disposition. *Proceedings of the eleventh international conference of the learning sciences* (*ICLS 2014*). ISLS, 23–27.
11. Clegg, T. et al. 2012. Technology for promoting scientific practice and personal meaning in life-relevant learning. *Proceedings of the 11th International Conference on Interaction Design and Children* (*IDC'12*). ACM Press, New York, NY, 152–161. DOI:https://doi.org/10.1145/2307096.2307114
12. Common Sense Media 2015. *Media Use By Tweens and Teens*. Common Sense Media, San Francisco, CA.
13. Diwanji, P. 2017. "Be Internet Awesome": Helping kids make smart decisions online. *Google*.
14. Doodle Jump: *http://www.limasky.com/*.
15. Doodle Jump Christmas Special APK: *https://apkpure.com/doodle-jump-christmas-special/com.lima.doodlejumpcs*.
16. Druin, A. 1999. Cooperative inquiry: developing new technologies for children with children. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (*CHI'99*). ACM Press, New York, NY, 592–599. DOI:https://doi.org/10.1145/302979.303166
17. Druin, A. 2002. The role of children in the design of new technology. *Behaviour & Information Technology*. 21, 1 (Jan. 2002), 1–25. DOI:https://doi.org/10.1080/01449290110108659
18. Excite-ed apps in stores now! *https://www.excite-ed.co.uk/news*.
19. Fails, J.A. et al. 2013. Methods and Techniques for Involving Children in the Design of New Technology for Children. *Foundations and Trends in Human–Computer Interaction*. 6, 2 (2013), 85–166. DOI:https://doi.org/10.1561/1100000018.
20. Federal Trade Commission. 2012. *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*. Federal Trade Commission. Washington, DC.
21. Federal Trade Commission. 2012. *Mobile Apps for Kids: Disclosures Still Not Making the Grade*. Federal Trade Commission. Washington, DC.
22. Federal Trade Commission. 2014. *Net Cetera: Chatting with Kids About Being Online*. U.S. Federal Trade Commission. Washington, DC.
23. Gee, J.P. 2007. *What video games have to teach us about learning and literacy*. Palgrave Macmillan, New York, NY.
24. Good Digital Parenting: *https://www.fosi.org/good-digital-parenting/*. Accessed: 2018-01-18.
25. Google. 2017. *Digital Citizenship & Safety Curriculum*. Google.
26. Guha, M.L. et al. 2013. Cooperative Inquiry revisited: Reflections of the past and guidelines for the future of intergenerational co-design. *International Journal of Child-Computer Interaction*. 1, 1 (Jan. 2013), 14–23. DOI:https://doi.org/10.1016/j.ijcci.2012.08.003.
27. Hartikainen, H. et al. 2016. Should We Design for Control, Trust or Involvement?: A Discourses Survey About Children's Online Safety. *Proceedings of the 15th International Conference on Interaction Design and Children* (*IDC'16*). ACM Press, New York, NY,

367–378.
DOI:https://doi.org/10.1145/2930674.2930680

28. Hipsky, S. & Younes, W. 2015. Beyond Concern: K-12 Faculty and Staff's Perspectives on Privacy Topics and Cybersafety. *International Journal of Information and Communication Technology Education*. 11, 4, (October-December 2015). 51-66. DOI:https://doi.org/10.4018/IJCTE.2015100104
29. Hodapp, E. 2010. "Doodle Jump" Halloween Update Adds Frankendoodler. *TouchArcade*.
30. Houde, S. & Hill, C. 1997. What do Prototypes Prototype? *Handbook of Human-Computer Interaction, Second edition*. M. Helander, T.K. Landauer, P. Prabhu, eds. Elsevier Science B.V., Amsterdam, Netherlands. 367–381.
31. Hourcade, J.P. et al. 2017. Child-Computer Interaction SIG: Ethics and Values. *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (*CHI'17*). ACM Press, New York, NY, 1334–1337. DOI:https://doi.org/10.1145/3027063.3049286
32. Hourcade, J.P. et al. 2016. Child-Computer Interaction SIG: New Challenges and Opportunities. *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (*CHI'16*). ACM Press, New York, NY, 1123–1126. DOI:https://doi.org/10.1145/2851581.2886433
33. King GAFA: 2017. https://www.kinggafa.com.
34. Klopfer, E. et al. 2009. *Moving learning games forward: Obstacles, opportunities, & openness*. MIT, Cambridge, MA.
35. Kumar, P. et al. 2017. "No Telling Passcodes Out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*. 1, CSCW (Dec. 2017), 1–21. DOI:https://doi.org/10.1145/3134699.
36. Lazzaro, N. 2004. Why We Play Games: Four Keys to More Emotion Without Story. *In Game Developers' Conference (GDC) 2004* (Mar. 2004).
37. Livingstone, S. 2006. Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. *Computers, Phones, and the Internet: Domesticating Information Technology*. R. Kraut, M. Brynin and S. Kiesler, eds. Oxford University Press, New York, NY. 145–167.
38. McNally, B. et al. forthcoming. Co-designing Mobile Online Safety Applications with Children. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (*CHI'18*). ACM Press, New York.
39. McReynolds, E. et al. 2017. Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (*CHI'17*). ACM Press, New York, NY, 5197–5207. DOI:https://doi.org/10.1145/3025453.3025735
40. Mindful Mountain: *https://beinternetawesome.withgoogle.com/interland/mindful-mountain*.
41. National Cyber Security Alliance. 2011. *The State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum.* National Cyber Security Alliance, Washington, D.C.
42. Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Palo Alto, CA.
43. Nolan, J. et al. 2011. The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media. *Journal of Childhood Studies*. 36, 2 (2011), 24–32. DOI:https://doi.org/10.18357/jcs.v36i2.15089.
44. Privacy Education: 2012. *https://www.fordham.edu/info/24071/privacy_education*. Accessed: 2018-01-18.
45. Prototyping on Paper: *https://marvelapp.com/pop/*.
46. Pruitt-Mentle, D. 2010. State of K12 Cyberethics, Safety and Security Curriculum in U.S.: 2010 Educator Opinion. National Cyber Security Alliance, Washington, DC.
47. Raynes-Goldie, K. and Allen, M. 2014. Gaming Privacy: a Canadian case study of a children's co-created privacy literacy game. *Surveillance & Society*. 12, 3 (Jun. 2014), 414–426.
48. Robin, B. 2006. The Educational Uses of Digital Storytelling. *Technology and Teacher Education Annual*. 1, (2006), 709–716.
49. Salen, K. and Zimmerman, E. 2003. *Rules of play: game design fundamentals*. MIT Press, Cambridge, MA.
50. Shribman, B. 2017. Introducing ideas of privacy while having fun. *Parenting for a Digital Future*.
51. Steeves, 2010. *Summary of Research on Youth Online Privacy*. Office of the Privacy Commissioner of Canada. Ottawa, Canada.
52. Steeves V. & Jones O. 2010. Surveillance, children and Childhood (Editorial). *Surveillance & Society*. 7, 3/4 (2010), 187–191.
53. Steinkuehler, C. et al. 2012. *Games, learning, and society: learning and meaning in the digital age*. Cambridge University Press, New York, NY.
54. Steinkuehler, C. and Squire, K. 2014. Videogames and learning. *The Cambridge handbook of the learning sciences*. R.K. Sawyer, ed. Cambridge University Press, New York, NY. 377–396.

55. Vitak, J. et al. 2018. SOUPS 2018 Designathon: Call for Participants. https://pearl.umd.edu/events/soups2018-workshop/. Accessed 2018-04-11.

56. Walsh, G. et al. 2013. FACIT PD: a framework for analysis and creation of intergenerational techniques for participatory design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (*CHI'13*). ACM Press, New York, NY, 2893-2902. DOI:https://doi.org/10.1145/2470654.2481400

57. Yip, J. et al. 2013. Brownies or bags-of-stuff?: domain expertise in cooperative inquiry with children. *Proceedings of the 12th International Conference on Interaction Design and Children* (*IDC'13*). ACM Press, New York, NY, 201–210. DOI:https://doi.org/10.1145/2485760.2485763

58. Zhang-Kennedy, L. et al. 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction*. 13, (Jul. 2017), 10–18. DOI:https://doi.org/10.1016/j.ijcci.2017.05.001.

59. Zhang-Kennedy, L. et al. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. *Proceedings of the 15th International Conference on Interaction Design and Children* (*IDC'16*). ACM Press, New York, NY, 388–399. DOI:https://doi.org/10.1145/2930674.2930716