2019

"Anon What What?": Children's Understanding of the Language of Privacy

Stacy Black
Boise State University

Rezvan Joshaghani
Boise State University

Dhanush Kumar Ratakonda
Boise State University

Hoda Mehrpouyan
Boise State University

Jerry Alan Fails
Boise State University

“Anon what what?”: Children’s Understanding of the Language of Privacy

Stacy Black
Rezvan Joshaghani
Dhanush kumar Ratakonda
stacyblack@u.boisestate.edu
RezvanJoshaghani@u.boisestate.edu
DhanushkumarRata@u.boisestate.edu
Computer Science Department
Boise State University
Boise, Idaho

Hoda Mehrpouyan
Jerry Alan Fails
hodamehrpouyan@boisestate.edu
jerryfails@boisestate.edu
Computer Science Department
Boise State University
Boise, Idaho

ABSTRACT

Internet usage continues to increase among children ages 12 and younger. Because their digital interactions can be persistently stored, there is a need for building an understanding and foundational knowledge of privacy. We describe initial investigations into children’s understanding of privacy from a Contextual Integrity (CI) perspective by conducting semi-structured interviews. We share results – that echo what others have shown – that indicate children have limited knowledge and understanding of CI principles. We also share an initial exploration of utilizing participatory design theater as a possible educational mechanism to help children develop a stronger understanding of important privacy principles.

IDC ’19, June 12–15, 2019, Boise, ID, USA

ACM ISBN 978-1-4503-6690-8/19/06…$15.00
https://doi.org/10.1145/3311927.3325324

CCS CONCEPTS

• **Social and professional topics** → **Children**; • **Human-centered computing** → Participatory design.

KEYWORDS

contextual integrity, privacy, security, children, participatory design

ACM Reference Format:
Stacy Black, Rezvan Joshaghani, Dhanush kumar Ratakonda, Hoda Mehrpouyan, and Jerry Alan Fails. 2019. "Anon what what?": Children's Understanding of the Language of Privacy. In *Interaction Design and Children (IDC '19), June 12–15, 2019, Boise, ID, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3311927.3325324

INTRODUCTION

The ubiquitous access to technology means that kids are using an increasing amount of technological devices and services. This can be a threat to their privacy and security, which is particularly troubling as they are a vulnerable population. Studies [4, 9] show that kids have limited understanding of privacy and security threats. The state-of-the-art theory of privacy is Contextual Integrity (CI), which defines privacy norms based on the context of information sharing. We performed an initial investigation based on CI that asked children to define words related to privacy and security, identify individuals with whom they feel comfortable sharing various personally identifiable information, and other questions. We also explore participatory design theater as a way to help children better understand these important privacy principles.

RELATED WORK

Research has been done on understanding young children's mental models regarding privacy, using Nissenbaum's theory of Contextual Integrity (CI) [1, 6] as a guiding principle [4, 9]. Under CI, a person's willingness to share information is dependent on attributes (the type of information), roles (the type of individual receiving the information), transmission principles, and contexts. Little research has been done on how children under the age of 11 recognize and cope with online privacy risks. Kumar et al. [4] attempted to help close the knowledge gap by asking how children view privacy and security, what strategies they use to protect themselves, and how parents help their children to protect themselves online. They found that while children understood that certain information types can be sensitive, they had trouble understanding transmission principles and context. Zhao et. al. [9] conducted a study to determine how children describe common privacy risks, and their risk response strategies for different risk contexts. They found that while children had a good understanding of *inappropriate content*, *the approach of strangers*, and *oversharing of personal information*, they had

Table 1: Child participant's names*, ages, and gender. (*Names are aliases; †Did not participate in semi-structured interview; ‡Did not participate in participatory design theater session)

Name*	Age	Gender	Group
Kate	7	Girl	G1
William†	7	Boy	G2
Darlene	8	Girl	G1
Victor‡	8	Boy	–
Mason	9	Boy	G1
Autumn‡	10	Girl	–
Kim	11	Boy	G2

a poorer understanding of *data tracking* and *online recommendations*. Further, the authors mention that current resources for keeping children safe online are mostly filtering or monitoring tools for parents, and parents feel poorly equipped to guide their children's use of digital technologies. However, neither of these studies looked specifically at how children share (or do not share) specific types of information with different roles.

To mitigate the risks discussed by the above studies, researchers propose that tools should be created to help children develop "big data" literacy, and research suggests that a scaffolding approach to learning [4, 5, 9] would be a useful approach to teach children how to protect themselves online. Several studies [5, 8] also demonstrate the usefulness of games and interactive stories to educate children about privacy. For example, Zhang-Kennedy et al. [8] designed an interactive e-book called "Cyberheroes" to teach children under the age of 10 about online privacy. In the story, the Cyberheroes must maintain their secret identities on the Internet. Researchers found that both parents and children enjoyed the book, and that the book was effective at teaching children about privacy risks. Kumar et al. [5] reviewed existing resources for teaching about online privacy. Of the types of resources they studied, they found that children enjoyed interactive games the most.

Using analogy and metaphors is another way to help children understand privacy concepts. Read and Beale [7] used Participatory Analogy to abstract complex topics to items and behaviors that children would be able to understand. They asked what young children (ages 8-9) considered "special" and what they would do to keep their most valuable item safe. The answers children gave researchers provided an idea of how a child might protect their personal information and passwords. Similarly, Participatory Analogy might be used to help teach children about complex privacy topics.

METHOD

Grounded from the perspective of CI, we wanted to investigate the understanding children have with regards to privacy concepts. We conducted a small pilot study consisting of a semi-structured interview, and a participatory design theater experience. Six children (age 7-11) participated in the interviews, five of the six participated in the participatory design theater experience (one was sick that day) to help us in this initial investigation. Their ages and genders are listed in Table 1.

Investigating Understanding via Semi-structured Interviews. The semi-structured interview conducted with children had three segments. The three segments consisted of asking children to define thirteen privacy-related words, what information they would share with various people, and some additional privacy questions (see Table 2). In our study, we assumed three contexts of family (parents, siblings and family friends roles), school (teacher, classmates roles), friends (close friends, friends, online friends roles), and neighbors.

After the three segments, we discussed in a full group the meanings of some of the words. During this debrief session, we all sat on the floor in a circle and asked children and adults to share their

Table 2: Child interview structure, with explanations about each segment.

Segment 1. Define thirteen privacy and security-related words to the best of their knowledge (See Figure 1). The words were chosen based on the common terminologies that are mostly used in the privacy and security aware tutorials and interactive books such as Cyberheroes [8]. The focus of the study was more on privacy threats related to data tracking.
Segment 2. What data they are comfortable sharing data (e.g., first name, full name, picture, etc.) with different roles (e.g., neighbors, family friends, online friends). The complete matrix (see Figure 2), few cells were grayed out for obvious reasons. This evaluates childrens' understanding of roles and information attributes in CI.
Segment 3. Additional questions to understand children's comfort in sharing information in a verbal conversation or through email/electronic media. We asked them to define privacy threats, security threats, and to share experiences with them. This evaluates childrens' understanding of transmission principles in CI.

Privacy Concept	Can Describe? Yes	No
Anonymity	0	6
Cyber crime	2	4
Cyber Disguise	2	4
Cyber Invisibility	2	4
Cyber trail	2	4
Data tracking	1	5
Digital Footprint	1	5
Encryption	0	6
Hacking	0	6
Pop-up	1	5
Scam	3	3
Secret	5	1
Secure connection	3	3

Figure 1: Privacy concepts that children were asked to define (to the best of their ability).

definitions to enable learning from one another and allow each individual to refine their understanding of the principle. Each child participant was interviewed by two researchers (one for taking notes and another for asking questions to children). The interviews lasted about 20 minutes each, and the group debrief afterwards was about 15 minutes.

The semi-structured interviews were audio-recorded, and the skits were video recorded. The semi-structured interviews were transcribed and analyzed using an inductive approach to develop codes [2, 3]. This is work in progress so further analysis is needed, but we share initial results. An author analyzed the transcriptions from segment one of the semi-structured indicating whether children accurately described the privacy concept or not (see Figure 1). Children's personal identifiable information (PII) sharing preferences for people with different roles were analyzed by counting how many said they would share that information with the corresponding role (see Figure 2). The responses for segment three were analyzed based on children's understanding regarding the risks of sharing information.

Participatory Design Theater to Learn Privacy. On a different day, children and adults were divided into two groups (each group having 2-3 children and 2-3 adults). Groups were asked to design and perform a skit on a privacy concept. Before dividing into groups, we had a large group discussion about three of the privacy terms from Figure 1: anonymity/cyber invisibility, digital footprint, and cyber disguise. These three concepts were chosen for the participatory design theater because there was a gap – based on our semi-structured interview and the related literature – in children's understanding of these concepts. One of these concepts was selected randomly by each group. The group then had 20 minutes to design and practice a skit about that concept. The skits were then presented to one another. The participatory design theater was viewed as a brief case-study and looked at with a qualitative lens.

RESULTS & FINDINGS

The results of our **semi-structured interview** illustrated that the children in our sample had little knowledge about privacy terminology. In *segment one* when researchers asked children to describe the privacy concepts, most of them were not able to describe them correctly (see Figure 1). Children mentioned that many of these concepts and terms were very new for them, some making clear it was the first time they had heard these words. The title for this submission for example comes from a child's response to the definition of *anonymous*, to which she responded "Anon what what?". Indeed, our results show there is a large gap in understand the contextual privacy among our participants and there is a need for work to lay a strong contextual privacy foundation.

Children's understanding of their contextual privacy with regards to roles and informational attributes was minimal. From the data obtained from the second segment of the semi-structured interviews helps us to understand their level of knowledge in sharing their PII (e.g., willingness to

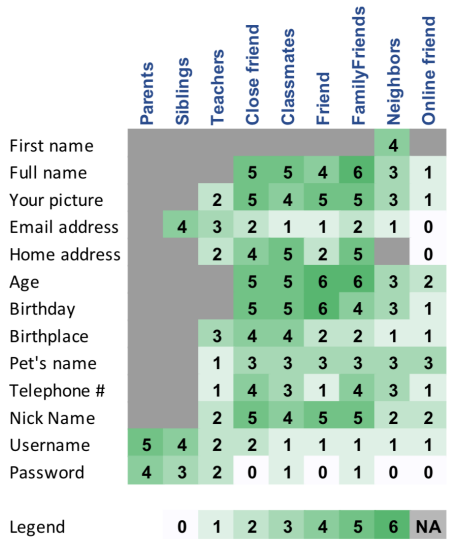

Figure 2: Children's personally identifiable information (PII) data sharing preferences with respect to those in different roles/relationships. Each cell contains the number of children (of 6) that would share that information with the corresponding person - a darker green means more would be willing to share that information. Gray cells indicate information that the role already has access to.

share information with an online friend). While there is an observed transition from roles with the most familiar relationship, there is not a lot of differentiation in terms of the kinds of information that they are willing to share. The majority of responses say that they are open to share their PII to someone from school (a classmate, a close friend, and a friend). Interestingly, they are willing to share their username and passwords with family, but not as much with those in other roles.

All the participants realized that sharing their personal information out-loud in a conversation is not safe. One participant said she would share her personal information with someone via email (Autumn), and another said he would write them on a piece of paper (Kim). In explaining why, the one said they knew the person they were sending the email to, and the other mentioned he could later destroy the paper and thus keep the information private. When we asked children "If a friend asks for your home address, are you comfortable sending it as an email or telling it to them?" three participants said they would tell them directly and two said they would send it in an email and one said she would not share her home address (which contradicted her response from segment two). For the same question, four participants (Victor, Darlene, Autumn, Kim) said they would not share their home address with their friend which contradicts their response in segment two.

Figure 2 shows that children have some understanding of the roles hierarchy, however, they are not consistent about their privacy decision with different roles and attribute types. Although their answers might indicate that they understand the privacy risks, their reasoning behind their responses might be flawed. For example, when Mason was asked if he was willing to share his home address with his classmates he said "yeah I could, they wouldn't really care, they wouldn't do anything, they don't even own a car." Regarding the kids understanding of transmission principles, it seems that kids have a harder time distinguishing the benefits and risks of different transmission methods. For example, Darlene said: "I would be more comfortable in email, because if you do it out loud you don't know if someone's watching or listening. It could go wrong."

In segment three we also asked them what is a *privacy threat* and *security threat*, to provide an example, and to share an experience they have had with these threats. All participants had a basic idea about privacy and security threats, though they had never experienced them online.

During the **participatory design theater session**, children formed two teams and chose randomly one of three privacy concepts to design and perform a skit. The children in the two groups (G1 and G2) are indicated in Table 1). G1 chose *Digital Footprints* from a bowl and they came up with a concept that all of them gets "sucked" into a black hole in a computer and as they walk around in the digital world inside the computer they left paper footprints Figure:3 that had personal information written on it like their email, home address, birthday, etc. They also had an *thief* role played by an author follow them and collect their paper/digital footprints. Some G1 participants gave their real date of birth and email address, but some included a fictional home address on their so-called *digital footprints* and said that "intruder is a bad person and she should not know our real personal information". One of

Figure 3: Children's "digital footprints" represented on paper footprints with personally identifiable information (PII).

ACKNOWLEDGMENTS

We thank the children who participated in this initial investigation who are a part of the intergenerational design team: Kidsteam at Boise State University. We thank NSF for supporting CISE-CRII-SaTC grant #1657774: A System for Privacy Management in Ubiquitous Environments.

the children, Kate, only included her initials on her digital footprints and said that "I don't want to leave my personal information."

G2 chose *Anonymity/Cyber Invisibility* and developed a skit where one participant wore an "invisibility bracelet" made out of paper on his wrist, which made him invisible to another person allowing him to follow others in a game and shopping cart and steal their items. William said the invisible person could add a product in Amazon and would be surprised when he saw another item which was not supposed to be in his cart when placing the order. They also discussed the possibility of being partially invisible so someone could see part of you.

In both skits, we saw a remarkable difference from the initial interviews when most could not clearly identify the meanings of terms, to some nuanced depth of understanding of the principles through the participatory design theater experience. We believe from this initial experience that this kind of an educational approach may be promising – although further investigations are warranted.

CONCLUSION & NEXT STEPS

With the use of technology now thoroughly embedded in children's daily lives, it is essential to adapt approaches that are child-centred to protect their online privacy and security, requiring further research. Our research illustrates the need for designing and developing child-friendly user interfaces, algorithms, and definitions that can provide children with the training and awareness required to stay safe online. Our findings confirm that further research with the considerations of the theoretical and methodological approaches are required to design and develop privacy security policies to reduce online risk. These policies will only be effective if we have an accurate understanding of how children's online activities intersect with their environment and their needs.

REFERENCES

[1] Adam Barth, Anupam Datta, John C Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: Framework and applications. (2006), 15–pp.

[2] Kathy Charmaz and Linda L. Belgrave. 2012. Qualitative interviewing and grounded theory analysis. *The SAGE Handbook of Interview Research: The Complexity of the Craft* (Jan. 2012), 347–366. DOI: http://dx.doi.org/10.4135/9781452218403.n25

[3] John W. Creswell. 1998. *Qualitative inquiry and research design: choosing among five traditions.* Sage Publications. Google-Books-ID: bjO2AAAAIAAJ.

[4] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 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: http://dx.doi.org/10.1145/3134699

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

[6] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

[7] Janet C Read and Russell Beale. 2009. Under my pillow: designing security for children's special things. (2009), 5.
[8] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* 13 (2017), 10–18.
[9] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Childs, Max Van Klee, and Nigel Shadbolt. 2019. I make up a silly name': Understanding Children's Perception of Privacy Risks Online. *arXiv preprint arXiv:1901.10245* (2019).