Toward a Practice-Based Approach to Privacy Literacy

Priya C. Kumar(✉)

Pennsylvania State University, University Park, PA 16802, USA
priya.kumar@psu.edu

Abstract. Children play, communicate, create, learn, and socialize with networked digital technologies. These activities generate data about what children do, where they go, and with whom they interact, raising questions about children's privacy. To help children understand and navigate such questions, information scholars and professionals advocate for privacy literacy efforts. Prior work builds on Nissenbaum's contextual integrity framework to define *what* privacy literacy is. In this paper, I link this prior work with theories of practice-based learning to begin explaining *how* educational efforts can help strengthen children's privacy literacy. Drawing on an example of a challenging incident described by an 11-year-old boy, I propose a practice-based approach to privacy literacy. I contend that educational efforts grounded in this approach will not only help children develop the skills they need to navigate privacy concerns, but also help them internalize the value of privacy.

Keywords: Children · Contextual integrity · Education · Online safety · Privacy

1 Introduction

Children play, communicate, create, learn, and socialize with networked digital technologies. These activities generate data about what children do, where they go, and with whom they interact, raising questions about children's privacy. To help children understand and navigate such questions, information scholars and professionals advocate for privacy literacy efforts [1–3]. In that vein, I have articulated privacy literacy as "the practice of enacting appropriate information flows within sociotechnical systems" [4]. I used the concepts of literacy as a social practice [5] and privacy as the appropriate flow of information [6, 7] as a foundation for defining *what* privacy literacy is. In this paper, I link that work with theories of practice-based learning [8] to begin explaining *how* educational efforts can help strengthen children's privacy literacy. Drawing on an example of a challenging incident described by an 11-year-old boy, I propose a practice-based approach to privacy literacy. I contend that educational efforts grounded in this approach will not only help children develop the skills they need to navigate privacy concerns, but also help them internalize the value of privacy.

M. Smits (Ed.): iConference 2022, LNCS 13192, pp. 135–142, 2022.
https://doi.org/10.1007/978-3-030-96957-8_13

2 Practice-Based Learning and Privacy Literacy

To develop literacy, one must learn. Learning involves acquiring knowledge, and effective education entails tapping into learners' motivations and fostering their ability to transfer knowledge to new situations [8]. Greeno et al. [8] describe three perspectives of learning that influence education. The behavioral/empiricist view treats learning as the transmission of information and skills that is reinforced through rewards and punishments. The cognitive/rationalist view considers learning as an intrinsically driven process of understanding concepts and developing abilities, such as problem solving. The situative/pragmatist-sociohistoric view regards knowledge as distributed across individuals, artifacts, and communities. Here, learning is a shared practice to which people contribute and through which they build identity. When people develop strong practice-linked identities, that is, when they have opportunities to connect closely with a practice, take on integral roles within it, and express themselves through it, they are more likely to actively engage with the practice [9]. One means of cultivating practice-linked identities is to craft experiences relevant to learners' everyday lives. For instance, designing and conducting food-related experiments with children can foster their identities as scientists and more actively engage them in science learning [10]. The situative/pragmatist-sociohistoric view is the most difficult for educators to put into practice, so to speak. But the upshot is learning experiences through which individuals connect knowledge to their own lives to the extent that it influences how they define themselves—a powerful educational outcome.

The purpose of privacy literacy efforts is to help children learn about privacy. Existing efforts embody the different perspectives of learning that Greeno et al. [8] articulate. What I have previously identified as the knowledge-based approach to privacy literacy [4] focuses on increasing people's awareness about institutional data management practices and teaching them to do things like change their privacy settings. Here, privacy literacy means knowing a set of facts, and the motivation for learning those facts is to gain the reward of protecting one's privacy (or risk losing it). In this way, the knowledge-based approach embodies a behaviorist/empiricist perspective of education. In contrast, researchers and practitioners in library and information studies have adopted a process-based approach to privacy literacy, which focuses on developing people's understanding of the contexts and implications of disclosing information online [3, 11]. Here, privacy literacy means thinking critically about a particular situation and making an informed choice. As such, the process-based approach aligns with the cognitive/rationalist perspective of education.

By defining privacy literacy as a practice of enacting appropriate information flows, I move privacy literacy toward the situative/pragmatist-sociohistoric perspective [4]. Practices are everyday routines embedded in particular contexts and often involving groups of people [12]. Practices are not just cognitive, but also social and cultural. When privacy is a practice, privacy is not a fact someone knows or a thought process in which someone engages, but an action someone does, often without conscious effort. Recognizing privacy as a practice aligns with broader shifts in privacy scholarship that treat privacy as a social, rather than individual, matter [6, 7].

Approaching privacy as a practice also complements sociotechnical shifts in the study of information literacy [12, 13]. Information literacy is not simply a set of discrete skills

and competencies pertaining to seeking and using information, but a social and cultural practice of meaning-making. The development of skills cannot be separated from the context in which it occurs, the social interactions that foster it, and the technologies that shape it. For instance, children gain privacy knowledge and skills from formal and informal learning environments, including school lessons and interactions with parents, siblings, relatives, and friends [2].

Indeed, while information literacy and online safety efforts often charge parents with monitoring or controlling children's online activities, parents are also a key source of support and guidance for children [14, 15]. Teachers and librarians are also well-positioned to incorporate privacy knowledge and skills into their interactions with children, which can reinforce and strengthen children's privacy literacy [1, 16]. Children can hone their data literacy, which includes recognizing the privacy implications of data collection, by participating in communities of practice. For example, children in the online programming community Scratch observed that the system displayed information about previous projects, reminding children of the persistence of information that in many cases they explicitly chose to display publicly [17]. In comments on projects and forum posts, children grappled with the privacy implications of such design decisions. Importantly, they engaged in these discussions on their own, unprompted by an adult trying to teach them a lesson [17]. This research on Scratch demonstrates how communities of practice offer meaningful opportunities to develop data literacy.

In summary, grounding privacy literacy in the situative/pragmatist-sociohistoric perspective of learning can yield educational efforts that not only help children develop practices to enact privacy in their everyday life, but also to help them internalize the value of privacy. To explain how, I draw on an example of challenging incident recounted by an 11-year-old boy and his mother and show how the experience can inform the development of a practice-based approach to privacy literacy.

3 Incident: Scammers on Instagram

As part of a larger project on how elementary school-age children conceptualize privacy online, I interviewed 18 families (23 parents and 26 children ages 5–11) about children's experiences with digital technologies [14]. When children described a situation that implicated privacy, I inquired further to explore how the child interpreted and handled the circumstances. One participant recounted a particularly salient experience. Ryan (a pseudonym) was 11 years old at the time of the interview and enjoyed playing mobile games such as Clash Royale. When asked if he had ever seen anything where people said things that made him feel uncomfortable or confused, he said, "I used to have Instagram and I saw some things. But, but those weren't inappropriate [things]. There were just people trying to get me to buy stuff…and they were, like, acting like my friend, like a kid or something."

A few years ago, when Ryan was 8 or 9, his family had returned to the U.S. after living abroad. Ryan set up an Instagram account to keep in touch with his friends. He said his Instagram profile was "open," and his mother added, "I knew nothing about Instagram then 'cause I wasn't on it, so I didn't know how to change the settings." Ryan and his friends enjoyed playing FIFA mobile soccer games, and Ryan posted about FIFA

on his Instagram. He explained that once, "I had gotten a good thing. So, I posted on my page the person I got. And then, so, like, so, a few FIFA scammers who wanted, like, coins and stuff. Yeah, they joined my thing. And they were talking to me like kids." They asked for his Xbox password, and though he didn't have an Xbox at the time, Ryan said, "I thought there might have been a password that my mom maybe…set up. So, I asked [my mom]."

His mother explained, "He just goes, 'Mom, Mom, can you give me the password of my Xbox and all these things, 'cause these people are going to give me cards.' And I was like, 'hold on a minute. Let's change your settings and, um, whatever.' But they were literally just trying to get information." When asked if he thought he would have disclosed the password, had he known it, Ryan replied, "Well, maybe when I was that age…I stopped completely sharing password when, like, I was around 10." Ryan's mother agreed, saying, "He would have given it [the password] in a heartbeat had he known it."

Later in the interview, Ryan's mother said that after the interaction, she discussed with Ryan that "these people aren't, you know, aren't probably being honest, and they're maybe trying to steal some information or money or buy things or you know, hack into your box, so, we never give the information out." She said she uses these organically arising moments to talk with her children about navigating online activities.

4 Understanding How Privacy Manifests in Children's Lives

To develop a practice-based approach to privacy literacy, it is important to understand how privacy manifests in children's everyday lives. Only then can information scholars and professionals craft privacy literacy efforts that truly resonate with children. I analyze the Instagram incident through the two theoretical frameworks that underpin a practice-based approach to privacy literacy: contextual integrity (CI) [6, 7] and situative/pragmatist-sociohistoric learning [8]. I specifically highlight how these frameworks attune adults to approach children's practices as valid, rather than flawed, even if they may lead to questionable outcomes. This attitude is critical because it frames privacy literacy as something adults can help children strengthen, rather than something adults need to fix in children.

CI contends that privacy arises when a given information flow follows the norms appropriate to its context. A privacy violation is then a misalignment between an information flow and the norms that it followed. Privacy norms are shaped by five parameters: information type, sender, recipient, subject, and transmission principle [7]. In the Instagram incident, the information type in question is the Xbox password. The sender would have been Ryan, and the recipient, the "FIFA scammers." The subject is the person to whom the information belongs, which in this case would have been Ryan's mother or whomever took ownership over the Xbox information. The transmission principle refers to the constraints that circumscribe an information flow. For example, Ryan believed that if he disclosed the Xbox password, his interlocutors would "give me cards," or materials useful for his FIFA gaming. In his mind, he would be offering a piece of information in return for useful materials, which suggests a transmission principle of exchange. However, his mother believed the people were "just trying to get information," potentially to steal money or break into systems, suggesting a transmission principle of exploitation.

Different transmission principles point to different outcomes—Ryan wanted to proceed with the information flow and his mother did not. Though it is impossible to know the true motives of the "FIFA scammers," Ryan's mother drew the more plausible conclusion that disclosing the password would result in harm. The Instagram incident supports conventional wisdom that parents should hide important passwords from children. However, this is not to suggest that Ryan's thinking was flawed.

When children and adults express conflicting desires, analysts are quick to attribute the differences to children's developmental immaturity and naïveté [18]. In this line of thinking, children do not yet possess the skills or life experience to make responsible decisions, but with time and guidance, they will hopefully learn to do so. This mindset is apparent in Ryan's own comments, as he noted that stopped sharing passwords as he grew older.

CI offers an alternative frame, one that does not approach children from a position of lack. Many adults would interpret Ryan's willingness to take the "FIFA scammers" at their word as demonstrating his lack of good judgment. Yet when the five parameters of the information flow, especially the transmission principle, are considered in context, his thinking becomes easier to understand. Ryan used Instagram as a way to keep in touch with his friends and participate in their shared interest of FIFA mobile gaming. For Ryan, Instagram operated in the context of friendship, where information often flows mutually and fosters close interpersonal bonds. This was the frame of reference through which Ryan interpreted the requests from the "FIFA scammers," and it explains why he perceived the requests as benign. In contrast, Ryan's mother recognized that Instagram also operates as a global interaction space where unfamiliar actors can intrude. She knew to approach unsolicited requests with skepticism and explained to Ryan that some people act with bad intentions. She predicted that the information flow, if allowed to occur, could violate privacy, and she used the incident as an opportunity to help her son understand what constitutes responsible online behavior.

Analyzing the Instagram incident through the CI framework provides insight into how seemingly risky actions can make sense to children. I now consider the incident through the situative/pragmatist-sociohistoric perspective of learning to illustrate why children might be motivated to engage in seemingly risky actions. This perspective approaches learning as a shared practice of building identity in community with others. Developing privacy literacy efforts from this perspective requires understanding:

- What are the social practices involved in navigating privacy?
- How do children participate in these practices?
- What identities do children develop through these practices?

Ryan used Instagram in the context of friendship, which involved engaging in the social practices of information disclosure and self-expression. Ryan and his friends connected over a shared enjoyment of FIFA, and he posted about his accomplishments in its mobile games. This not only informed his friends about his progress in the games, but also represented an aspect of his identity.

Ryan participated in these practices by leveraging the affordances of Instagram. He followed his friends and posted content relevant to them. As long as his friends also followed him, his content would automatically appear on their feeds. This reduced the

effort he had to expend to share information with his friends, but it also meant that he had less awareness of who precisely saw what he posted. Since Instagram only recently began defaulting youth users to a private profile [19], Ryan likely did not consciously decide to make his content publicly visible. But the consequence was that he, perhaps unwittingly, opened himself up to interactions with people beyond his friends.

Ryan said "a few FIFA scammers… joined my thing. And they were talking to me like kids." This suggests that people began following his account and trying to communicate with him, either by commenting on his posts or sending him direct messages. According to Ryan, the messages appeared to be coming from other children and offered him game perks in exchange for an Xbox password. The messages tapped into both aspects of identity development linked to Ryan's Instagram use—his identity as a friend and as a FIFA gamer—which can explain why the requests to share his password resonated with Ryan.

5 Future Directions for Developing Practice-Based Privacy Literacy

Analyzing the Instagram incident through the theoretical frameworks of CI and pragmatist-sociohistoric learning demonstrate how practices that seem obviously risky to adults can make sense to young children. This is important because it frames children's actions as valid, rather than naive or wrong. Practice-based privacy literacy focuses on equipping children to understand and reflect on their actions in the context of social, rather than purely individual, well-being. Here, enacting privacy is not simply about protecting oneself, but about contributing positively to a community of practice. For example, in the Instagram incident, Ryan's mother could have emphasized that a compromised Xbox could have put Ryan's friends and fellow FIFA gamers at risk by bringing unauthorized parties into their games.

Given the importance of community and identity in practice-based learning, privacy literacy efforts will need to be grounded something other than privacy. For example, Clegg et al. [10] promoted science learning by creating a program about cooking and embedding scientific concepts into the activities. Similarly, educators could promote privacy literacy by creating programs that appeal to children's interests (e.g., creating a successful YouTube channel), and embedding privacy concepts into the program content.

Practice-based privacy literacy does not seek to instruct children about the correct ways to interact online nor to prevent children from experiencing challenging situations. It aligns with Wisniewski's [20] resilience-centered approach to online safety, which moves away from parental control and prioritizes helping youth develop self-regulation strategies to cope with risky situations when they inevitably encounter them. One way that educational efforts can promote resilience is by leveraging the persuasive power of stories. People regularly share stories when interacting with friends and family, and when such stories involve security-related decisions, hearing them can shape how people think and act when they encounter a situation that implicates their security [21]. Children already glean privacy knowledge from friends and family [2], so a privacy literacy effort could help children use their experiences (or those they hear from others) to craft and exchange privacy-related stories. To embed this effort within a community of practice,

researchers could partner with an after-school coding club or a makerspace, work with children to identify how privacy manifests in their coding or making practices, and help children craft and present stories about their experiences navigating privacy.

I invite information scholars and professionals, along with experts in privacy, learning science, education, and child development, to build on this foundation and design educational experiences that help children understand and navigate privacy questions. Specifically, future work should identify the communities of practice children engage in and the identities they develop within these communities, explore how the practices in these communities implicate privacy, and devise meaningful activities, including but certainly not limited to storytelling, that truly resonate with children's lives.

Acknowledgements. I thank Tammy Clegg for introducing me to the learning sciences and for inspiring my thinking in this paper.

References

1. Chi, Y., Jeng, W., Acker, A., Bowler, L.: Affective, behavioral, and cognitive aspects of teen perspectives on personal data in social media: a model of youth data literacy. In: Chowdhury, G., McLeod, J., Gillet, V., Willett, P. (eds.) iConference 2018. LNCS, vol. 10766, pp. 442–452. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78105-1_49
2. Subramaniam, M., Kumar, P., Morehouse, S., Liao, Y., Vitak, J.: Leveraging funds of knowledge to manage privacy practices in families. Proc. Assoc. Inf. Sci. Technol. **56**, 245–254 (2019). https://doi.org/10.1002/pra2.67
3. Wissinger, C.L.: Privacy literacy: from theory to practice. Commun. Inf. Lit. **11**, 378–389 (2017)
4. Kumar, P.C., Subramaniam, M., Vitak, J., Clegg, T.L., Chetty, M.: Strengthening children's privacy literacy through contextual integrity. Media Commun. **8**, 175–184 (2020). https://doi.org/10.17645/mac.v8i4.3236
5. Scribner, S., Cole, M.: The Psychology of Literacy. Harvard University Press, Cambridge (1981)
6. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford (2010)
7. Nissenbaum, H.: Contextual integrity up and down the data food chain. Theoret. Inq. Law. **20**, 221–256 (2019). https://doi.org/10.1515/til-2019-0008
8. Greeno, J.G., Collins, A.M., Resnick, L.B.: Cognition and learning. In: Berliner, D.C., Calfee, R.C. (eds.) Handbook of Educational Psychology, pp. 15–46. Macmillan Library Reference USA, Simon & Schuster Macmillan; Prentice Hall International, New York, London (1996)
9. Nasir, N.S., Hand, V.: From the court to the classroom: opportunities for engagement, learning, and identity in basketball and classroom mathematics. J. Learn. Sci. **17**, 143–179 (2008). https://doi.org/10.1080/10508400801986108
10. Clegg, T.L., Gardner, C.M., Kolodner, J.L.: Playing with food: moving from interests and goals into scientifically meaningful experiences. In: Proceedings of the 9th International Conference of the Learning Sciences, pp. 1135–1142. International Society of the Learning Sciences (2010)
11. Rotman, D.: Are you looking at me?—Social media and privacy literacy. In: Proceedings of the iConference 2009, pp. 1–3. iSchools, Chapel Hill (2009)
12. Tuominen, K., Savolainen, R., Talja, S.: Information literacy as a sociotechnical practice. Libr. Q. **75**, 329–345 (2005). https://doi.org/10.1086/497311

13. Lloyd, A.: Information Literacy Landscapes: Information Literacy in Education, Workplace and Everyday Contexts. Chandos, Oxford (2010)
14. Kumar, P., Naik, S.M., Devkar, U.R., Chetty, M., Clegg, T.L., Vitak, J.: "No telling passcodes out because they're private": understanding children's mental models of privacy and security online. Proc. ACM Hum.-Comput. Interact. **1**(CSCW), 1–21 (2017). https://doi.org/10.1145/3134699
15. Subramaniam, M., Valdivia, C., Pellicone, A., Neigh, Z.: Teach me and trust me: creating an empowered online community of tweens and parents. In: Proceedings of the 2014 iConference, pp. 244–258 (2014). https://doi.org/10.9776/14078
16. Kumar, P.C., Chetty, M., Clegg, T.L., Vitak, J.: Privacy and security considerations for digital technology use in elementary schools. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI 2019, pp. 1–13. ACM Press, Glasgow (2019). https://doi.org/10.1145/3290605.3300537
17. Hautea, S., Dasgupta, S., Hill, B.M.: Youth perspectives on critical data literacies. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 919–930. ACM, New York (2017). https://doi.org/10.1145/3025453.3025823
18. Castañeda, C.: Figurations: Child, Bodies, Worlds. Duke University Press, Durham (2002)
19. Instagram: Giving Young People a Safer, More Private Experience (2021). https://about.instagram.com/blog/announcements/giving-young-people-a-safer-more-private-experience
20. Wisniewski, P.: The privacy paradox of adolescent online safety: a matter of risk prevention or risk resilience? IEEE Secur. Priv. **16**, 86–90 (2018). https://doi.org/10.1109/MSP.2018.1870874
21. Rader, E., Wash, R., Brooks, B.: Stories as informal lessons about security. In: Proceedings of the Eighth Symposium on Usable Privacy and Security – SOUPS 2012, p. 1. ACM Press, Washington, D.C. (2012). https://doi.org/10.1145/2335356.2335364