COGITATIO

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 175–184
DOI: 10.17645/mac.v8i4.3236

Article

Strengthening Children's Privacy Literacy through Contextual Integrity

Priya C. Kumar [1,*], Mega Subramaniam [1], Jessica Vitak [1], Tamara L. Clegg [1] and Marshini Chetty [2]

[1] College of Information Studies, University of Maryland, College Park, MD 20742, USA;
E-Mails: pkumar12@umd.edu (P.C.K.), mmsubram@umd.edu (M.S.), jvitak@umd.edu (J.V.), tclegg@umd.edu (T.L.C.)
[2] Department of Computer Science, University of Chicago, Chicago, IL 60637, USA; E-Mail: marshini@uchicago.edu

* Corresponding author

Submitted: 7 May 2020 | Accepted: 13 July 2020 | Published: 10 November 2020

Abstract
Researchers and policymakers advocate teaching children about digital privacy, but privacy literacy has not been theorized for children. Drawing on interviews with 30 families, including 40 children, we analyze children's perspectives on password management in three contexts—family life, friendship, and education—and develop a new approach to privacy literacy grounded in Nissenbaum's contextual integrity framework. Contextual integrity equates privacy with appropriate flows of information, and we show how children's perceptions of the appropriateness of disclosing a password varied across contexts. We explain why privacy literacy should focus on norms rather than rules and discuss how adults can use learning moments to strengthen children's privacy literacy. We argue that equipping children to make privacy-related decisions serves them better than instructing them to follow privacy-related rules.

Keywords
children; contextual integrity; digital technology; learning moments; password management; privacy education; privacy literacy; transmission principles

Issue
This article is part of the issue "Children's Voices on Privacy Management and Data Responsibilization" edited by Ralf De Wolf (Ghent University, Belgium) and Mariek Vanden Abeele (Tilburg University, The Netherlands).

1. Introduction

Researchers and policymakers advocate integrating privacy into information literacy efforts to help children understand the privacy implications of digital activities (Culver & Grizzle, 2017; Stoilova, Nandagiri, & Livingstone, 2019). However, current approaches to privacy literacy focus too narrowly on privacy as control (Hagendorff, 2018) and have not been theorized for children. By interpreting children's perspectives on password management through the contextual integrity (CI) framework (Nissenbaum, 2010, 2019), we ground privacy literacy in a well-established privacy theory and connect it to children's experiences of privacy.

Media and communication studies treats privacy literacy as knowledge to be learned (Bartsch & Dienlin, 2016; Baruh, Secinti, & Cemalcilar, 2017; Park, 2013; Park & Jang, 2014; Trepte et al., 2015), while library and information studies regards privacy literacy as a process of critical thinking (Rotman, 2009; Wissinger, 2017). Instead, we draw on literacy as a social practice (Scribner & Cole, 1981) and privacy as the appropriate flow of information (Nissenbaum, 2010, 2019) to articulate privacy literacy as the practice of enacting appropriate information flows within sociotechnical systems. In this article, we interpret children's perspectives on password management in three contexts—family life, friendship, and education—through the CI framework and explain why privacy literacy should attend to norms rather than rules. We also discuss how adults can use learning moments to help strengthen children's privacy literacy.

2. Related Work

To lay the groundwork for our approach to privacy literacy, we identify the limitations of current conceptu-

alizations of privacy literacy. We then review how the CI framework treats privacy, explaining why it holds promise for privacy literacy. We subsequently situate our approach to privacy literacy within existing research on children's digital privacy.

2.1. Privacy Literacy

Existing conceptions of privacy literacy focus on the individual dimension of privacy. The knowledge-based approach to privacy literacy distinguishes between factual/declarative knowledge (e.g., knowing that apps collect data) and procedural knowledge (e.g., knowing how to limit this data collection; Trepte et al., 2015). Surveys operationalize factual/declarative knowledge through true/false or yes/no questions about data collection and management practices, and procedural knowledge through self-report questions about familiarity or comfort with tasks like adjusting privacy settings or turning off location tracking (Bartsch & Dienlin, 2016; Park, 2013; Park & Jang, 2014). However, given that most American adults report low levels of privacy knowledge (Auxier et al., 2019), relying on knowledge alone may not be a practical way to help people protect their privacy. And as technologies and interfaces change, facts and procedures quickly grow obsolete, requiring constant updates to privacy knowledge.

The process-based approach to privacy literacy includes five components: understanding contexts of information disclosure, recognizing where information is shared, realizing the implications of disclosing private information, evaluating potential privacy threats, and deciding what to disclose (Rotman, 2009). Here, privacy literacy is a form of critical thinking (Wissinger, 2017). While this approach acknowledges the dynamic nature of privacy management, it focuses narrowly on the disclosure of private information. A conception of privacy literacy grounded more broadly in the flow of information would equip people to evaluate a wider field of privacy concerns (Hagendorff, 2018).

To expand privacy literacy beyond individual decisions about disclosing information, we find Scribner and Cole's (1981) account of literacy as a social practice a useful starting point. They argue literacy "is not simply knowing how to read and write…but applying this knowledge for specific purposes in specific contexts of use" (Scribner & Cole, 1981, p. 236). Literacy involves developing particular skills and understanding when, why, and how to enact those skills. This implicates more than individual abilities, as social contexts, cultural norms, expert authorities, and institutional policies all shape the practice of literacy.

2.2. Privacy as Contextual Integrity

Technology and media scholar Helen Nissenbaum (2010, 2019) devised the CI framework to explain how sociotechnical systems threaten privacy. CI does not equate privacy with secrecy or control but with the appropriate flow of information. That is, privacy is about ensuring that information travels in socially acceptable ways. For example, imagine two friends, where Friend 1 has a love interest but declines to tell Friend 2 who it is. Friend 2 demands that Friend 1 disclose the love interest's name or the friendship is over. Friend 1 reluctantly reveals the name. A CI analysis explains why this violates Friend 1's privacy.

CI posits that information flows appropriately when the flow aligns with the norms of a particular context. To conduct a CI analysis, one must first identify whether an information flow aligns with contextual informational norms. They must then evaluate the flow against the broader ethical and moral commitments of society to determine whether any norm violations rise to the level of unacceptability. Defining the norms that govern a specific information flow requires identifying five parameters: the type of information involved, the information subject (i.e., to whom the information belongs or refers), the sender, the recipient, and the transmission principles (i.e., constraints imposed on the information flow). Table 1 identifies parameters for the example information flow.

This information flow occurs in the context of friendship, where people typically share freely within the bounds of companionship. While a transmission principle of mutuality usually circumscribes the friendship context, the example flow involved coercion, where Friend 2 compelled Friend 1's disclosure by threatening the relationship's existence. The change in transmission principles goes against contextual norms. But pronouncing this a privacy violation requires evaluating the flow against societal values. Coercion is not antithetical in the context of friendship; if Friend 1 withheld the location of someone in imminent danger, Friend 2 could justifiably impel disclosure. But forcing Friend 1 to reveal a love interest's name rattles the trust that binds friendships. Social

Table 1. Parameters of information flow.

Parameter	Example Information Flow
Information type	Love interest's name
Information subject	Friend 1
Sender	Friend 1
Recipient	Friend 2
Transmission principle	Coercion

fabric would fray if friendships resembled depositions. Consequently, by altering the transmission principle of the information flow, Friend 2 undermined its contextual integrity and violated Friend 1's privacy. The transmission principle "may be the most distinguishing element of the framework of contextual integrity; although what it denotes is plain to see, it usually goes unnoticed" (Nissenbaum, 2010, p. 145). No definitive list links specific transmission principles with contexts; instead, the "possibilities for constraints that may serve as [transmission principles] are endless" (Nissenbaum, 2019, p. 230).

While primarily intended to inform the design and regulation of technologies, CI could be a useful foundation for privacy-related educational efforts. CI does not dictate how information should flow; it offers a method for making privacy-related decisions. CI could help children identify information flows, recognize the contextual norms that govern flows, and evaluate whether flows are appropriate. This approach would *equip* rather than instruct children; it would help them learn how to manage privacy rather than teach them what to do to protect privacy.

2.3. Children and Digital Privacy

Research about children's digital privacy typically focuses on older children and interpersonal dimensions of privacy (Stoilova et al., 2019). Many children over age 10 report knowing how to change social media privacy settings (Livingstone, Mascheroni, Ólafsson, & Haddon, 2014) but demonstrate less understanding of how data flows implicate privacy (Bowler, Acker, Jeng, & Chi, 2017; Selwyn & Pangrazio, 2018). Questions of children's privacy vis-à-vis commercial and institutional data practices remain understudied (Stoilova et al., 2019), though one experimental study found that watching a video about online data practices increased children's (knowledge-based) privacy literacy related to the commercial use of data (Desimpelaere, Hudders, & Van de Sompel, 2020). Children receive little privacy-related instruction, with educators uncertain about what it should entail (Culver & Grizzle, 2017) or believing younger children do not need it (Kumar, Chetty, Clegg, & Vitak, 2019).

Nevertheless, children recognize aspects of how online interactions affect privacy (Kumar et al., 2017). Families draw on several non-school sources of knowledge, including informal learning experiences, advice from relatives and friends, and information from expert sources, to navigate privacy online (Subramaniam, Kumar, Morehouse, Liao, & Vitak, 2019). Children can develop data and privacy literacy through participation in online communities (Hautea, Dasgupta, & Hill, 2017) or design workshops (Selwyn & Pangrazio, 2018). Research recommends that privacy education efforts clearly relate to children's everyday lives (rather than present contrived or irrelevant scenarios) and give children opportunities to practice decision-making (Kumar et al., 2018; Raynes-Goldie & Allen, 2014). Children, like adults, move through a variety of social contexts, but existing approaches to privacy literacy do not explore how contextual norms affect privacy. To address this, we contribute a new conception of privacy literacy based on an analysis of children's password management practices in three contexts—family life, friendship, and education.

3. Methods

We draw on interviews we conducted with families as part of two projects about privacy, security, and everyday digital technology use. One project, which examined how children conceptualize privacy and security online, involved 18 families (23 parents and 26 children ages 5–11; Kumar et al., 2017). The second project, which focused on how low-income families navigate digital privacy and security concerns, included 52 families (54 adults and 23 children, ranging from toddlers to adult age; Subramaniam et al., 2019). We did not collect age or other demographic information from participants in the second project, though they often volunteered such information during the interviews. We made this decision because low-income individuals may have less trust in researchers, and given the sensitive nature of our interview questions, we wanted to avoid making participants uncomfortable by asking about their demographics. For more information about this decision, see Vitak, Liao, Subramaniam, and Kumar (2018).

In both projects, we asked children and parents about children's experiences with digital devices, inquiring further if they mentioned privacy, security, or related concepts (e.g., secrecy). In the first project, we also played a game with children where we presented hypothetical scenarios (e.g., a sibling looking at the screen while a child plays on a tablet) and asked how they would recommend a child handle the situation. Interviews for both projects occurred across the U.S. state of Maryland between December 2016 and June 2017. We interviewed each family once. In the second project, some families included relatives such as grandparents. We use the term parent in this article to refer to a child's primary caregiver, which can encompass various kinship or other relations. When reporting participant quotes, we label participants from the first project with a letter and those from the second with a number.

Both research teams developed codebooks based on their research goals and revised them as they coded transcripts (King, 2014). For this article, we selected codes related to privacy and security for further analysis. While reviewing the interview excerpts, we observed that children's responses to questions about privacy often echoed this 10-year-old boy's: "Just don't tell your password and username or any…private things" (Family W). This rule linking privacy to the secrecy of a password permeated the interviews, with children attributing it to parents and teachers alike.

Since children connected passwords with privacy, we decided to focus on information flows related to pass-

word management. We identified relevant excerpts from interviews with 30 families, including 40 children. This encompassed all 18 of the families from the first project and 12 families from the second project (14 adults and 14 children). To analyze the data, we first drew diagrams depicting the information flows involving passwords. This attuned us to the various practices involved in password management (e.g., knowing, remembering, forgetting, discerning, and disclosing passwords) and to the contexts in which children managed passwords. Following CI, we then clustered excerpts by practice and context, identified the parameters of information flows, and parsed participants' determinations of appropriateness.

4. Findings

Children's password management practices spanned three contexts: family life, friendship, and education. Children encountered passwords while accessing devices (e.g., computer, Chromebook, tablet, smartphone) and accounts (e.g., games, social media, school). We organize the findings by context and interpret children's perspectives surrounding a specific information flow—the disclosure of passwords—through CI, highlighting connections to privacy literacy.

4.1. Family Life Context: Knowing, Forgetting, and Discerning Passwords

The family life context encompassed password practices among parents, children, and siblings. In some cases, passwords did not flow from parents to children, suggesting parents did not regard children as appropriate recipients of passwords. A 7-year-old surmised his mother refused to disclose a password so he and his siblings "don't get into her computer when she's not looking"; his 9-year-old brother added that "she doesn't really want us playing on the computer all the time" (Family C). A 6-year-old said she tried to get her mother to reveal her phone's passcode "so when she's like, in the shower, I can get onto it" (Family K). A 7-year-old said she was going to try and figure out her mother's Kindle password and her mother replied, "Oh please don't, you'll lock both of us out if you do that" (Family D).

Other children said parents told them passwords on the condition that they not tell others. Two adults chided children for disclosing passwords during the interview. One told her 8-year-old grandson, "You don't tell your passwords ever, to any of those, unless you tell meemaw [colloquial term for grandmother]. I'm the only one that's supposed to know other than your teacher, okay?" (Family 12). In CI terms, this caregiver suggested a transmission principle of notice—telling the grandparent—before reverting to one of confidentiality—that only a (grand)parent or teacher should know a password.

Another parent, whose 5-year-old son disclosed his family's iPad password to the interviewer, said she had likened passwords to door keys to explain to her son why "a password isn't something that you can share with everybody….We just don't leave keys lying around for the door…[because] anyone can find them and break in." She suggested that circumstantial factors could have made him feel comfortable disclosing the password during the interview: "Maybe he really trusts you [the interviewer]…because you're in our house….Maybe, somebody on the street, he may not do it" (Family S). The boy may have regarded the interaction as governed by the transmission principle of mutuality, treating the interviewer as a friend whom he could trust with the password, or of requirement, treating the interviewer as an authority figure whose presence in his home demanded knowledge of the password.

Passwords did not flow reciprocally between parents and children; while parents could withhold passwords from children, they often required children to disclose any passwords they managed to parents. As one 8-year-old boy explained, "My mom knows my password, and that's the first person I need to tell because she always needs to know my password" (Family H). Some children expressed interest in keeping their parents out of their devices. A 7-year-old said she would not want her mother to know her tablet's password "because I don't want my mom getting on my iPad and seeing what her future birthday presents [are]" (Family D).

Children's recollections also underscored parents' important role in helping children manage passwords. Some children needed assistance remembering passwords; one 8-year-old girl said, "My mom usually makes a password for me and puts it on a piece of paper so I can remember it, and it's usually, like, in the coupon box" (Family G). Other families suffered the consequences of children's forgetfulness. A 10-year-old wanted a password for her iPad because "I didn't like it when a lot of people just went on my iPad" (Family Y). She "made a passcode when [my parents] weren't around and then I forgot it and we had to, like, back up the whole iPad and re-download a bunch of apps and stuff." Another parent said her 6-year-old daughter "creates email addresses and passwords like it's nothing. She probably has a million of them. I'll find papers around the house that have…all these different characters and letters" (Family 4). This highlights that privacy literacy efforts must also consider children's evolving developmental capacities.

Password flows also varied between siblings. An 11-year-old said she told her 8-year-old sister her email password (Family V). Others deduced siblings' passwords or vice-versa. One 9-year-old "figured out my brother's password on his phone and I didn't tell him for two days." He revealed his deed on the third day after his brother "said 'if you figure out the password then I'll let you play on it.'" He guessed the password by using the numbers in his brother's phone number (Family 7). An 11-year-old said he changed his phone's password from four to six digits after his 8-year-old brother fig-

ured it out. During the interview, the younger boy said he overheard his brother tell their mother to "double the thing," and disclosed what he thought the new password was. "Now I have to change it again," the older brother replied (Family B). Indeed, while the targeted sibling may feel annoyed or concerned that the perpetrating sibling might mess up their device or account, such experiences may also be necessary for children to learn privacy norms (Wolfe & Laufer, 1975).

Families understandably differed in their beliefs about who constituted an appropriate recipient of a password. These decisions were influenced in part by children's abilities and dispositions relating to, for instance, remembering a password or limiting their time spent playing computer games. Password management also involved play and transgression, for example, nonchalantly creating accounts or cleverly deducing a sibling's password. These are typical aspects of child behavior. While adults may want to correct these seemingly negative actions, we should also consider how these actions help children develop richer, more nuanced understandings of privacy.

4.2. Friendship Context: Trust, or Lack of it

Children were usually told not to disclose passwords to others, with secrecy or confidentiality as the underlying transmission principle. Discussions about password sharing among friends or generic 'other people' invoked other transmission principles. For example, a 7-year-old said she disclosed her iPad password to a neighbor, whom she called a "grownup friend…because she needed [the password]," though she didn't remember why (Family F). Here, the transmission principle of requirement superseded that of confidentiality. An 11-year-old said he felt comfortable sharing game passwords with friends if doing so could help him in the game, invoking the transmission principle of exchange—each party benefits from the information flow (Family B). When asked whether a child should share an account password with a friend, one 10-year-old girl said it depended on the friend:

> If it's someone that you don't know very well or that you aren't really close to, then I wouldn't do it. But, like, sometimes if me and my friends are working together and she wants to look something up on my Chromebook and [she's] my really close friend who I trust, I just tell her my password and she tells me her password and like….I know that she's not going to tell anyone else because I trust her. (Family Y)

This girl invoked the transmission principle of mutuality, evaluating the appropriateness of the flow in part based on whether she trusted the recipient. Some participants said children should only disclose passwords to parents, while others mentioned that children may not want to reveal passwords to anyone. One 11-year-old called the disclosure a privacy issue; her 8-year-old sister added, "Sometimes, you have things that you don't want to tell people, even your parents" (Family V), returning to the transmission principle of secrecy.

Children explained that disclosing a password to a friend could lead to negative outcomes, such as someone telling others the password, looking at personal accounts, or doing something on the device or account that could get the child in trouble. An 8-year-old boy said that if the person asking for the password was "a stranger, maybe they could post something bad [about] our friends and then our friends wouldn't like us anymore just because of them" (Family P).

Indeed, when the conversation turned to disclosing passwords to non-friends, children deemed such flows inappropriate. Some said they wouldn't disclose their passwords because, as one 8-year-old boy put it, "I don't like people messing up my games" (Family B). A 6-year-old said he shouldn't disclose his Animal Jam password because "if they steal your phone….They could do bad stuff on it like, they could tell people what they didn't want to actually tell" (Family N). An 8-year-old girl explained:

> I wouldn't let anyone else use my password because it's my password. It's my personal business, not theirs….If someone gets my password, maybe they would use it for something that I didn't do and I might get in trouble for something I didn't do. And I don't wanna risk [that]. And I don't want anyone to know my personal business. If that password may be connected to any of my personal family business or any of my business, then I don't want anyone to be looking into it and finding out any of my own stuff. (Family G)

A critical interpretation could construe these children as reciting online safety tropes they've likely heard before. But reading their explanations through CI points to ways of discussing privacy with children beyond online safety. Children said disclosing passwords to non-friends could result in privacy violations (someone seeing information you don't want them to see), reputational harm (someone posting negative content about you), and getting in trouble (if the person does something bad or inappropriate while using your accounts). However, children also acknowledged that disclosing passwords with friends could yield benefits or reinforce intimacy (Marwick & boyd, 2014).

4.3. Education Context: Challenges to Protecting Passwords

The education context encompassed password practices among teachers, students, and classmates. Children said teachers gave students their passwords, often written on a card. An 8-year-old said his teacher kept the cards "for safekeeping" (Family A). An 8-year-old girl said students can memorize their passwords but keep their cards in

their desk in case they forget (Family G). One 6-year-old called his school password "secret" (Family X), and several children said they were not allowed to share school passwords. However, one 6-year-old said her teacher allowed her to share her password with a classmate who lacked her own account (Family C). Here, we see the transmission principle shift from secrecy, suggesting the password should not be disclosed at all, to one of consent, where the password can be disclosed if the teacher permits the student to do so.

In other cases, passwords could be inferred. A 7-year-old said her initials served as the password for a school math game, meaning classmates knew each other's passwords (Family Q). Her mother added, "The passcode is just to [track] their progress though, it's not like they get access to anything else," implying that the password's weakness posed little concern. A 10-year-old said his school's passwords used students' birthdays and nobody had gotten into his account "because I didn't tell anyone my birthday" (Family I).

Rules against password sharing did not prevent students from trying to discern others' passwords. A 6-year-old girl said that when students use index cards to log into their accounts, "they're supposed to cover [it with] their hand…and not look….I type my…passcode in fast so [classmates] won't know, but then they still know it because they peek at it" (Family C). An 11-year-old said students in his district received six-digit passwords; his 8-year-old brother said students sometimes "type random numbers and then get into someone's account" (Family B). He suspected that happened to him when he noticed that his account's profile image had changed from a penguin to a bicycle. He said he told his teacher, "so she told, like, the principal and then they made an announcement, like, no hacking." When asked if he had to change his password, he replied, "No, they don't like me to change the passwords."

Other children said their schools offered options to change passwords. One eleventh grader said her school used students' birthdays as passwords, adding that "you didn't have to change it, but it was an option" (Family 13). She said that while she learned about "safety precautions" in school, this included "nothing about passwords." A 10-year-old boy explained that at the beginning of the school year, students have the option of changing their passwords; "right before, we'll do a video that's [about] how to make a good password" (Family W).

Some children did not consider information flows that involved others accessing their school materials problematic. An 8-year-old justified disclosing her school password to an interviewer because "you don't really get to any of our private information by a Chromebook" (Family G). A 7-year-old expressed little worry about others looking on his school computer because "everybody in my class has the same [information on their Chromebooks]" (Family C). While the presence of platforms like Google in classrooms has rightly raised privacy concerns (Kumar et al., 2019), these children did not seem to share such concerns. Considering the education context from a child's viewpoint may help explain why. Children are required to go to school, follow the schedules set out for them, complete the tasks assigned to them, and submit their work for evaluation. Younger children in particular experience little autonomy over the information on their Chromebooks, so they may find it appropriate for that information to flow to others, even if it sits behind a password.

5. Discussion

Based on our analysis of children's perspectives of password management practices in three contexts, we explain why strengthening children's privacy literacy requires focusing on norms rather than rules. One way adults can strengthen children's privacy literacy is by taking advantage of learning moments to discuss privacy norms with children.

5.1. From Rules to Norms

While rules and norms shape behavior, rules "tend to be explicit and emanate from authoritative sources," whereas norms emerge, vary, and shift more flexibly than rules (Nissenbaum, 2019, p. 227). CI's parameters of information flows—subject, sender, receiver, information type, and transmission principle—provide a rich set of variables for dissecting norms, while rules flatten information flows to one or two parameters, obscuring others. Rules like 'don't tell anyone your password' ascribe secrecy to the password. Secrets refer to information that is hidden, typically because it could reflect negatively on someone. Passwords are not secrets in this sense; they require protection not because of what they mean but because of what they do—control access. In CI terms, secrecy equals the stoppage of information flows, but children did not experience passwords as secret.

A more fitting transmission principle is confidentiality, which "focuses on relationships" and "involves trusting others to refrain from revealing personal information to unauthorized individuals" (Richards & Solove, 2007, p. 125). Rules like 'don't tell anyone except a parent or teacher your password' imply confidentiality with their reference to those who typically hold the position of trusted adult in children's lives. Children's responses surfaced additional transmission principles that govern information flows involving passwords, including requirement (disclosing a password because someone needs it), exchange (disclosing because you'll receive something in return) and mutuality (disclosing as a form of relational intimacy).

These principles implicate trust, raising questions like, do you trust this person needs the password? Do you trust that disclosing a password will yield the promised benefit? Do you trust that your friend won't mess up your account? While children may implicitly consider these questions when deciding whether to disclose a password,

efforts to strengthen children's privacy literacy should make this questioning explicit. Rather than tell children what is or is not private, educational efforts should help children determine when information should or should not flow in a particular situation.

We do not suggest abandoning rules; indeed, their clarity and simplicity can scaffold learning and skill development, especially for younger children. But we propose that adults connect rules to norms and discuss rules in terms of contextually appropriate information flows. The rule 'don't tell anyone your password' becomes 'only disclose your password to someone you trust.' For younger children, rules can define trusted recipients, such as parents, close friends, or teachers until children recognize how to evaluate trust. As children grow, rules evolve.

CI gives adults and children a vocabulary to discuss the positive and negative implications of information flow. For instance, a few children expressed comfort telling a close friend a password. In CI terms, this flow could be appropriate because it supports close relations between peers, an important societal priority. As children grow, privacy literacy's objectives shift from helping children understand the rationale behind rules to helping them recognize what makes certain information flows more appropriate than others. Applied to password management, this means that as children gain experience in different social contexts, privacy literacy becomes less about their knowing why they shouldn't disclose a password (rule) and more about their ability to make decisions about disclosing a password (norm).

5.2. Using Learning Moments to Strengthen Children's Privacy Literacy

One way to integrate privacy literacy into children's everyday lives could be through identifying learning moments. Consider Family S, where a 5-year-old boy disclosed an iPad password to an interviewer even though his mother had told him passwords should be guarded like house keys. She could have presumed her son forgot or didn't understand her advice. Instead, she suggested he might have trusted the interviewer. Rather than viewing her son's behavior as wrong, she considered the situation from his perspective and recognized how he could have perceived the information flow to be appropriate.

This kind of thinking can attune caregivers and educators toward opportunities for learning moments to discuss appropriate privacy behavior. One could imagine the Family S parent asking her son why he disclosed the password to the interviewer and the two collaboratively generating scenarios when it would and would not be appropriate to disclose passwords. Talking through scenarios in connection with examples from children's lived experience can concretize the abstract concept of norms for children. Conversely, one could imagine a parent chiding a child for breaking the 'no telling passwords' rule, which also occurred in our interviews. Where attending to norms can promote inquiry with children, enforcing rules leaves little room for conversation.

This CI-based approach can also help adults consider what types of privacy lessons will resonate with children. For instance, some children did not express concern at others viewing their Chromebook information. The differing norms that govern the education and family life contexts can explain why children might not question those information flows. In addition, some school password practices went against security best practices. Thus, while school is an obvious place for children to learn about privacy, such lessons might be more effective if they discuss privacy flows in non-education contexts. In other words, a lesson on password security might resonate more if it uses the example of protecting a game account rather than a school account. This also underscores the value of reinforcing privacy lessons across different social contexts (Kumar et al., 2019).

Grounding privacy literacy in appropriate norms does not mean ceding responsibility for information flows to children. Parents may want to know a child's password so they do not have to reset a device if/when the child forgets it. Teachers may write student passwords on index cards because helping children reset their passwords if/when they forget them consumes valuable instruction time. Practices that seem to contradict general privacy and security advice make sense in context, particularly when considering children's evolving cognitive, social, and emotional development. Indeed, any attempt to strengthen children's privacy literacy must accommodate variations in children's developmental capacities, caregivers' child-rearing approaches, educators' pedagogical styles, policies of institutions like schools, affordances of digital platforms, and privacy regulations pertaining to children's data. While recent work has begun to develop privacy-related guidance for children of different ages (Prior & Renaud, 2020), we believe CI offers a means to address several of these variations because of its commitment to norms over rules and its attendance to privacy as the appropriate flow of information.

6. Conclusion

Drawing on discussions about children's password management practices in 30 families, we offer a new approach to privacy literacy grounded in CI (Nissenbaum, 2010, 2019). We recognize this type of privacy education requires more effort than giving children a rule to follow, and we encourage further participatory work with children, caregivers, and educators to translate CI into age-appropriate forms. But oversimplifying privacy as a property of information (i.e., passwords are private) or reducing it to a set of black-and-white rules (i.e., don't tell anyone your password) does children a disservice because it does not take into account their lived experiences with information management. Framing privacy as a set of rules centers children's compliance rather than their skill development. We argue for strengthening children's pri-

vacy literacy not in terms of teaching them rules but by helping them enact appropriate information flows. The latter will better equip them for the information management tasks they will face as they get older.

Acknowledgments

We thank our family participants for their time and contributions as well as Andrea Castillo and Shalmali Naik for their assistance conducting the interviews. We also thank the editors of the thematic issue and the anonymous reviewers for their feedback. The first project discussed in this article was funded by a Google Faculty Research Award, and the second project was funded by an IMLS National Leadership Grant (LG-81–16-0154–16). No one from either organization was involved in the research.

Conflict of Interests

The authors declare no conflict of interests.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Washington, DC: Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bowler, L., Acker, A., Jeng, W., & Chi, Y. (2017). "It lives all around us": Aspects of data literacy in teen's lives. *Proceedings of the Association for Information Science and Technology*, *54*(1), 27–35. https://doi.org/10.1002/pra2.2017.14505401004

Culver, S. H., & Grizzle, A. (2017). *Survey on privacy in media and information literacy with youth perspectives*. Paris: UNESCO. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000258993

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, *110*, 1–12. https://doi.org/10.1016/j.chb.2020.106382

Hagendorff, T. (2018). Privacy literacy and its problems. *Journal of Information Ethics*, *27*(2), 127–145.

Hautea, S., Dasgupta, S., & Hill, B. M. (2017). Youth perspectives on critical data literacies. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 919–930). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3025453.3025823

King, N. (2014). Using templates in the thematic analysis of text. In C. Cassell & G. Symon (Eds.), *Essential guide to qualitative methods in organisational research* (pp. 256–270). Newcastle: SAGE.

Kumar, P. C., Chetty, M., Clegg, T. L., & Vitak, J. (2019). Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3290605.3300537

Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (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*. https://doi.org/10.1145/3134699

Kumar, P., Vitak, J., Chetty, M., Clegg, T. L., Yang, J., McNally, B., & Bonsignore, E. (2018). Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children* (pp. 67–79). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3202185.3202735

Livingstone, S., Mascheroni, G., Ólafsson, K., & Haddon, L. (2014). *Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile*. London: London School of Economics and Political Science.

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Nissenbaum, H. (2019). Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law*, *20*(1), 221–256. https://doi.org/10.1515/til-2019-0008

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303. https://doi.org/10.1016/j.chb.2014.05.041

Prior, S., & Renaud, K. (2020). Age-appropriate password "best practice" ontologies for early educators and parents. *International Journal of Child–Computer Interaction*, *23/24*, 1–12. https://doi.org/10.1016/j.ijcci.2020.100169

Raynes-Goldie, K., & Allen, M. (2014). Gaming privacy:

A Canadian case study of a children's co-created privacy literacy game. *Surveillance & Society*, *12*(3), 414–426.

Richards, N. M., & Solove, D. J. (2007). Privacy's other path: Recovering the law of confidentiality. *Georgetown Law Journal*, *96*(1), 123–182.

Rotman, D. (2009). Are you looking at me? Social media and privacy literacy. In *Proceedings of the iConference 2009*. Grandville, MI: iSchools.

Scribner, S., & Cole, M. (1981). *The psychology of literacy*. Harvard, MA: Harvard University Press.

Selwyn, N., & Pangrazio, L. (2018). Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data & Society*, *5*(1), 1–12. https://doi.org/10.1177/2053951718765021

Stoilova, M., Nandagiri, R., & Livingstone, S. (2019). Children's understanding of personal data and privacy online: A systematic evidence mapping. *Information, Communication & Society*. Advance online publication. https://doi.org/10.1080/1369118X.2019.1657164

Subramaniam, M., Kumar, P., Morehouse, S., Liao, Y., & Vitak, J. (2019). Leveraging funds of knowledge to manage privacy practices in families. *Proceedings of the Association for Information Science and Technology*, *56*(1), 245–254. https://doi.org/10.1002/pra2.67

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Dordrecht: Springer. https://doi.org/10.1007/978-94-017-9385-8

Vitak, J., Liao, Y., Subramaniam, M., & Kumar, P. (2018). 'I knew it was too good to be true": The challenges economically disadvantaged Internet users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. *Proceedings of the ACM on Human-Computer Interaction*, *2*. https://doi.org/10.1145/3274445

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy*, *11*(2), 378–389.

Wolfe, M., & Laufer, R. (1975). The concept of privacy in childhood and adolescence. In S. T. Margulis (Ed.), *Man-environment interactions: Evaluations and applications* (Vol. 6, pp. 29–54). Stroudsburg, PA: Halsted Press.

About the Authors

Priya C. Kumar is a Doctoral Candidate at the University of Maryland's College of Information Studies (iSchool), where she examines how the datafication of everyday life reshapes privacy, especially for parents and children. Priya holds an MS in Information from the University of Michigan and BA degrees in Journalism and Government and Politics from the University of Maryland. Find out more about her research at https://www.priyakumar.org

Mega Subramaniam (PhD) is an Associate Professor and the Co-Director of the Youth eXperience (YX) Lab at the College of Information Studies (iSchool) at the University of Maryland. She received her PhD in Information Studies from Florida State University and her MA in Instructional Systems Technology from Indiana University, Bloomington. Dr. Subramaniam's research focuses on enhancing the role of public libraries in fostering the mastery of emerging digital literacies among underserved young people.

Jessica Vitak (PhD) is an Associate Professor in the College of Information Studies at the University of Maryland. She is a subject matter expert in data privacy, surveillance, and ethics, and her research examines the social and ethical implications of big data and empowers people through education and tools that help them make more informed decisions when using technology. Read more about her research at https://pearl.umd.edu

Tamara L. Clegg is an Associate Professor in the College of Information Studies and the Department of Teaching and Learning, Policy and Leadership at the University of Maryland. Her work focuses on developing technology to support life-relevant learning where learners engage in STEM experiences in the context of achieving personally relevant goals.

Marshini Chetty is an Assistant Professor in the Department of Computer Science at the University of Chicago. She specializes in human–computer interaction, usable privacy and security, and ubiquitous computing. Her work has won best paper awards at SOUPS, CHI, and CSCW, and she was a co-recipient of the Annual Privacy Papers for Policymakers award. Her research has been funded by the National Science Foundation, the National Security Agency, Facebook, and multiple Google Faculty Research Awards.