The Contextual Integrity Framework as an Educational Tool

Priya Kumar
University of Maryland
College Park, MD 20742, USA
pkumar12@umd.edu

Abstract
In this paper, I describe how my colleagues and I used Nissenbaum's contextual integrity (CI) framework as an analytical lens to explore how children ages 5-11 conceptualize privacy online. I then consider whether CI can be an educational tool to help children develop privacy decision-making skills. This departs from CI's primary focus of informing the design or evaluation of technologies, as well as the policies that govern their use. But it could bring the theory to new constituencies, including children, parents, and educators.

Author Keywords
Contextual integrity; privacy decision-making; children; parents; educators

CSCW '18 Workshop: Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design, Nov. 3 – 7, 2018, Jersey City, New Jersey.

ACM Classification Keywords
• **Security and privacy** → **Human and societal aspects of security and privacy** → Social aspects of security and privacy

Introduction: CI as a Versatile Tool for Privacy Research
In the five years since I first read Nissenbaum's "Privacy in Context," [7] I've used the contextual integrity (CI) framework to study a snarky parenting blog, people's perceptions about data flows from wearable fitness trackers, and children's understanding of privacy online [3]. These projects focused on various technologies and social practices, and each engaged with CI in a different way.

Like many, I see CI as a versatile tool for privacy research. Beyond its utility as a conceptual and analytical framework around which to structure a study or analyze data, CI can help translate social understandings of privacy into technical aspects of digital systems. CI's attendance to the ethical and moral implications of the normalization of certain data flows lend it the power to persuade decision makers to act a certain way or to justify decisions related to information flows.

Yet scholars are typically not using CI to its full potential. Research in human-computer interaction (HCI) using CI tends to reference the framework as a motivation for addressing a given research problem; fewer studies employ it as a tool for designing a study or analyzing data [1]. Computer science research using CI considers context from a situational rather than social perspective, and it does not address the normative dimensions of CI [2].

Keeping these critiques in mind, I want to explore CI's potential as an educational tool to help children develop skills to navigate privacy and security online. This departs from CI's primary focus as a framework to evaluate existing information flows and to inform the design of technologies (and the policies that govern their use). But I believe it presents a promising direction for the theory to resonate with new constituencies: children, parents, and educators.

Inspiration: CI as a Tool for Understanding Children and Privacy Online

The idea of using CI as an educational tool grew out of the aforementioned project about children and privacy online. With colleagues at the University of Maryland and Princeton, I interviewed 18 families – 26 children ages 5-11 and 23 of their parents – about how children used digital devices and how they navigated (or imagined navigating) any concerning situations online.

After using CI to analyze our data, we saw that children typically understood how *actors* and *attributes* could affect privacy online, but that children under age 10 did not discuss how *transmission principles* affected privacy online [4]. In addition, children relied largely on their parents to help them handle unfamiliar situations online, while parents generally did not feel that their children encountered privacy or security concerns online. Based on these findings, we advocated for the development of educational materials that use the CI framework as an organizing principle to teach children privacy-related concepts. We also recommended the creation of materials that equip parents to scaffold their children's understandings of privacy online.

To get a better sense of what types of educational materials could help children learn about privacy online, our team conducted three co-design sessions with a team of children ages 8-11. We determined that educational materials should go beyond framing privacy management as a set of "do's and don'ts" and instead help children develop the skills to make decisions related to privacy and security online [5]. Educational materials alone cannot convey the contextual, nuanced nature of privacy management, but they can prompt children to have conversations about the topic with peers, parents, educators, and other trusted adults.

To understand how school experiences affect children's privacy online, we conducted focus groups with elementary school educators. We found that while educators consider aspects of privacy and security when using technology in the classroom, they rarely discuss digital privacy and security with their students.[1]

Through this project, we aim to highlight opportunities across the home and school contexts to help children develop privacy decision-making skills. In this spirit, I offer the following provocation for the CSCW workshop: can we use the CI framework as the foundation from

[1] Our paper reporting these findings is under review.

which to scaffold children's privacy decision-making skills?

Provocation: CI as a Tool for Privacy Education

Literature reviews show that researchers in computer science and HCI rarely take up the normative dimensions of CI [1,2]. Yet this is where the framework derives its persuasive power. A new information flow may violate the norms of a particular context, but the violation may be justified if done in the name of a moral or political value, such as justice. Conversely, if a new information flow violates contextual integrity in ways that are unacceptable according to moral or political values, there may be grounds to rethink, change, or eliminate that information flow [7].

Admittedly, this oversimplifies CI, and rarely are the circumstances we study so straightforward to characterize. But a similar approach could be used to teach children privacy decision-making skills in a way that acknowledges the nuanced and context-dependent nature of privacy while still offering a practical and teachable way to *think through* that nuance.

Consider how Nissenbaum & Patterson [8] applied CI to self-tracking practices in a workplace context. After describing *context*, *actors*, *attributes*, and *transmission principles* at play, they conducted a normative evaluation of the practice at three levels:

1. Whose and what interests are at play;
2. What ethical and political values are implicated;
3. How the ends and values of the context are affected.

Based on this evaluation, they offered architectural, legal, and policy suggestions to help address the privacy risks that emerge from self-tracking practices in the workplace.

Nissenbaum & Patterson [8] presented a sophisticated analysis; I am not suggesting that we try to teach elementary school children to do the same. Rather, I propose that teaching children to identify the *context*, *actors*, *attributes*, and *transmission principles* at play in a given scenario, to consider the implications of information flows, and to compare them against moral, political, or ethical values can equip them to navigate privacy in an increasingly interconnected world.

For example, one study suggests that children are comfortable with parents monitoring location information from a child's mobile device, since parents are responsible for a child's physical safety [6]. What about granting location access to another actor in another context, for example, an augmented-reality mobile game like Pokémon Go or a social media app like Snapchat? Entertainment and socializing may not appear to implicate ethical or political values. But conversations about whether it is appropriate to share location information with these actors could discuss the decision from the perspective of fairness (e.g., is it fair for data to be the "price" of using an app) or transparency (e.g., do people understand what the company or other actors do with location information).

Our team is actively considering what CI-based educational tools could look like. One idea is a child-friendly ad blocker, a browser extension that helps children learn about who "watches" them online. The system could then prompt children to reflect on the

fairness question posed in the previous paragraph. Another idea is a choose-your-own-adventure storytelling app in which characters make privacy-related decisions in different contexts (e.g., home, doctor's office, library). A teacher could have students interact with the app and then discuss how and why privacy-related decisions differ across contexts.

Approaching privacy education from a CI perspective can show children that privacy is not about following instructions (e.g., never share location information) or knowing the right answers; it is about considering a situation and deciding what one feels comfortable doing. The children in our study showed evidence of understanding how the parameters of CI affect norms of information flow, even if they did not use CI's terminology [4]. Given this, developing educational materials or technologies to help children learn to apply the CI framework to their own privacy decisions may not be as far-fetched as it seems.

Acknowledgements

I thank my collaborators on the children and privacy online project, especially Marshini Chetty, Tammy Clegg and Jessica Vitak. This project was supported by a Google Faculty Research Award. No one from Google was involved in the research.

References

1. Karla Badillo-Urquiola, Xinru Page, and Pamela Wisniewski. 2018. Literature Review: Examining Contextual Integrity within Human-Computer Interaction. 1–4. Paper presented at the Symposium on Applications of Contextual Integrity.
2. Sebastian Benthall, Seda Gürses, and Helen Nissenbaum. 2017. Contextual Integrity through the Lens of Computer Science. *Foundations and Trends® in Privacy and Security* 2, 1: 1–69. https://doi.org/10.1561/3300000016
3. Priya Kumar. 2018. Contextual Integrity as a Conceptual, Analytical, and Educational Tool for Research. 1–5. Paper presented at the Symposium on Applications of Contextual Integrity.
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: 1–21. https://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. 67–79. https://doi.org/10.1145/3202185.3202735
6. Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing Mobile Online Safety Applications with Children. 1–9. https://doi.org/10.1145/3173574.3174097
7. Helen Nissenbaum. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA.
8. Helen Nissenbaum and Heather Patterson. 2016. Biosensing in Context: Health Privacy in a Connected World. In *Quantified : biosensing technologies in everyday life*. MIT Press, Cambridge, London, 79–100.