Contextual Integrity as a Conceptual, Analytical, and Educational Tool for Research

Priya Kumar
College of Information Studies
University of Maryland
College Park, Maryland, USA
pkumar12@umd.edu

ABSTRACT

Helen Nissenbaum's contextual integrity (CI) framework is a popular and versatile tool for studying the privacy implications of various technologies and practices, including social media, wearable fitness trackers, and children's understanding of privacy. Yet meta-reviews find that studies using CI do not engage with the entire framework, neglecting to consider their findings against society's prevailing moral or political values. My colleagues and I have used CI as a conceptual tool to shape research questions and as an analytical tool to interpret data. We are also exploring CI's potential as an educational tool to help children develop privacy decision-making skills. However, these applications of CI possess the same limitation that meta-reviews highlight. In this paper, I describe my applications of CI and consider how engaging with the framework as a whole could strengthen their contribution.

CCS CONCEPTS

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

KEYWORDS

Contextual integrity; privacy; social media; wearable fitness trackers; children; education

ACM Reference format:

P. Kumar. 2018. Contextual Integrity as a Conceptual, Analytical, and Educational Tool for Research. Presented at the *Symposium on Applications of Contextual Integrity, Princeton, New Jersey USA, September 13-14, 2018 (PrivaCI '18)*, 5 pages.

PrivaCI'18, September 13-14 2018, Princeton, New Jersey, USA

1 INTRODUCTION

One summer morning five years ago, my family and I pulled into a rest stop while traveling for vacation. I had just finished a chapter of Nissenbaum's "Privacy in Context" [7] and was imagining how the contextual integrity (CI) framework could inform my nascent master's thesis project on parents, social media use, and privacy. I tried to explain my enthusiasm as we waited for coffee, but my parents could only nod politely, not quite understanding how context, attributes, actors, and transmission principles could elicit such excitement.

Though I did not end up using CI in my thesis, I've applied it in three distinct research projects examining social media, wearable fitness trackers, and children's understanding of privacy. CI is a popular and versatile tool for studying privacy, but meta-reviews find that studies using CI do not engage with the entire framework [1, 2]. Specifically, studies neglect to consider information flows against society's prevailing moral or political values. My applications of CI also possess this limitation. In this paper, I describe my three applications of CI and consider how engaging with the entire CI framework could strengthen the contributions of these projects. Before describing my work, I briefly review the framework itself.

2 A REVIEW OF THE CONTEXTUAL INTEGRITY FRAMEWORK

Contextual integrity holds that privacy is the "right to ***appropriate*** flow of personal information" [7:127, emphasis in original]. Appropriate flows are those that align with context-specific norms and ethical values, and thus conform to people's expectations. Determining the appropriateness of information flows involves identifying the ***context*** in which a particular action or practice occurs, the ***actors*** involved, the ***attributes*** of the information in play, and the ***principles of transmission*** that dictate how that information flows. A technology that changes information flows or creates new ones does not automatically raise privacy concerns. But a technology that causes information to flow in ways ***that are not appropriate to the context*** very well may. The CI framework holds that these new or altered information flows should be evaluated against the context's prevailing moral or political values. If the information flow contradicts these values, there may be a strong argument to modify or even abandon the technology [7:190-191].

3 THREE APPLICATIONS OF THE CONTEXTUAL INTEGRITY FRAMEWORK

3.1 Unexpected Social Media Information Flows

My dissertation research examines the privacy implications of parents posting pictures of their children online. To understand what emerging norms shape this practice, I analyzed a sample of posts from STFU, Parents,[1] a snarky blog that aims, in part, to serve "as a guide for parents on what NOT to post [online] about their kid" [3]. The blog publishes screenshots of content that parents have shared on social media (with names and faces redacted) and critiques them. I found that the blog implored parents to consider how social media posts could affect their self-presentation rather than how disclosing information about children online could affect privacy [4]. But evaluating these norms, and the blog that espouses them, through the lens of CI

[1] The blog's name stands for "Shut the F*ck Up, Parents" and is available at http://stfuparentsblog.com.

reveals how the practice can raise privacy concerns. The blog publishes screenshots of social media content without the awareness (or permission) of the person who posted the content, which means its very existence presents an unexpected information flow and a potential violation of ***transmission principles***. The blog takes content disclosed in one ***context***—family life— and presents it in another—entertainment. In addition, the blog prioritizes the interests of particular ***actors***— the social media audience—over those of the parent or child.

In this study, CI served as a conceptual lens that helped me make sense of gaps I saw in the data – namely, the blog's lack of attention to privacy as a consideration related to social media use. I could take this analysis further by identifying the interests of various actors (e.g., social media users, social media companies, parents, children) and evaluating them against values such as fairness or informational self-determination. This would help answer the question of whether the practice of parents posting pictures of their children online is problematic, and if so, what should be done about it.

3.2 Privacy Expectations Over Time

As part of a broader project about privacy and mobile technology use, colleagues from the University of Maryland, University of Wisconsin-Milwaukee, and I interviewed people who use fitness trackers. We combined our data with interviews that Heather Patterson conducted with different Fitbit users in 2013 [8,9] with the goal of exploring how user attitudes toward data sharing changed from 2013 to 2017.[2]

Here, CI served as the conceptual framework that inspired the study as well as the analytical framework through which we interpreted the data. Conceptually, our goal for this study was to consider the central component of CI – the appropriateness of a particular information flow – and how judgments of it change over time. Analytically, we examined our data by clustering participant quotes based on the degree to which they expressed comfort with a particular information flow and then interpreting the quotes to see what transmission principles informed participants' perspectives.

Our findings suggest that over time, people are more willing to consider a particular information flow as appropriate. At the same time, their evaluation becomes more nuanced, focusing on the purpose of an information flow or what transmission principles apply rather than a simpler consideration of context. For example, this means asking why an employer needs personal fitness information and whether an employer deserves personal fitness information rather than simply deciding that personal fitness information should not be shared in an employment context.

If users themselves increasingly take an "it depends" stance to the question of whether a particular information flow is appropriate, how are technology developers, policymakers, and others whose decisions affect people's privacy supposed to make those decisions? Fleshing out this analysis through the ethical, political, and moral dimensions of the CI framework could shed light on this question.

3.3 Children's Understanding of Privacy Online

In another project with colleagues at the University of Maryland and Princeton, I interviewed children

[2] Our paper on this study is in progress.

ages 5 to 11 and their parents to understand how children conceptualize privacy online [5]. We did not approach the project with the goal of applying the CI framework, but we realized during data analysis that children's comments often invoked one of the framework's aforementioned four parameters. Here, we used CI to evaluate children's awareness of how privacy plays out online. We found that children generally understood how ***actors*** and ***attributes*** affect privacy online, but that those under age 10 struggled to understand the role of ***transmission principles***.

Our team then held co-design sessions with children ages 8-11 to explore how games and storytelling can be used to develop educational resources to teach elementary school-aged children about privacy online [6]. We found that such resources should move beyond instructing children about the "do's and don'ts" of managing privacy and instead help children develop the skills they need to make informed decisions related to privacy online. CI's focus on serving as a heuristic to help people pinpoint privacy concerns and mitigate them suggest that it can also be a valuable tool for privacy education. But it is important for such efforts to harness the complete framework, since the act of examining an information flow against a society's prevailing moral or political values is what allows for the determination that it raises privacy concerns.

4 CONCLUSION

In this paper, I described how colleagues and I applied the contextual integrity framework to studies of social media, wearable fitness trackers, and children's understanding of privacy. These projects cover a variety of data types and research questions. They show the breadth of cases to which CI applies and highlight CI's value as a conceptual and analytical tool to support the research process. The third project, which suggests that CI can also be a useful tool to teach people about privacy, broadens the audience for this framework beyond policymakers and technology developers to include educators.

However, these applications of CI primarily focused on the first part of the framework — identifying how ***context***, ***actors***, ***attributes***, and ***transmission principles*** influence norms, expectations, or understandings of privacy. This means they possess the same limitation that meta-reviews of applications of CI have highlighted [1,2] – they neglect the higher levels of the CI framework that involve considering information flows against society's prevailing moral or political values. I described how engaging with the entire framework could strengthen these studies, a reflective exercise that I have found helpful and would recommend to other researchers who seek to realize the full potential of the CI framework.

ACKNOWLEDGMENTS

I thank my collaborators on the projects described here: Jessica Vitak, Yuting Liao, Tammy Clegg, Elizabeth Bonsignore, Brenna McNally, Shalmali Naik, and Utkarsha Devkar from the University of Maryland; Marshini Chetty and Jonathan Yang from Princeton; Michael Zimmer and Katie Kritikos from the University of Wisconsin-Milwaukee, and Heather Patterson from Intel. I also thank Marshini Chetty, Helen Nissenbaum, and Yan Shvartzshnaider for organizing this symposium. Finally, I thank Helen Nissenbaum for developing the CI framework, which has resonated with me as a scholar and individual living in the digital age.

REFERENCES

[1] Badillo-Urquiola, K, Page, X., & Wisniewski, P. 2018. Literature Review: Examining Contextual Integrity within Human-Computer Interaction. Presented at the Symposium on Applications of Contextual Integrity (Princeton, NJ, 2018), 1–4.

[2] Benthall, S., Gürses, S., & Nissenbaum, H. 2017. Contextual Integrity through the Lens of Computer Science. *Foundations and Trends® in Privacy and Security* 2, 1 (2017), 1–69. https://doi.org/10.1561/3300000016.

[3] Koenig, B. n.d. About the blog: *http://www.stfuparentsblog.com/about*. Accessed: 2017-08-06.

[4] Kumar, P. 2018. Emerging Norms and Privacy Implications of Parental Online Sharing: The Perspective of the STFU, Parents Blog. Presented at the 68th Annual Conference of the International Communication Association (Prague, Czech Republic, 2018), 1–30.

[5] Kumar, P. et al. 2017. "No Telling Passcodes Out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*. 1, CSCW (Dec. 2017), 1–21. DOI:https://doi.org/10.1145/3134699.

[6] Kumar, P. et al. 2018. Co-Designing Online Privacy-Related Games and Stories with Children. *Proceedings of the 2018 Conference on Interaction Design and Children* (Trondheim, Norway, 2018), 67–79. DOI: https://doi.org/10.1145/3202185.3202735.

[7] Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

[8] Patterson, H. 2013. Contextual Expectations of Privacy in Self-Generated Health Information Flows. Presented at TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy (Arlington, VA, Mar. 2013), 1–48.

[9] Patterson, H. and Nissenbaum, H. 2013. Context-Dependent Expectations of Privacy in Self-Generated Mobile Health Data. Presented at the Privacy Law Scholars Conference (Berkeley, CA, Jun. 2013), 1–52.