Media and Communication

Open Access Journal | ISSN: 2183-2439

Volume 8, Issue 4 (2020)

Children's Voices on Privacy Management and Data Responsibilization

Editors

Ralf De Wolf and Mariek Vanden Abeele

COGITATIO

Media and Communication, 2020, Volume 8, Issue 4
Children’s Voices on Privacy Management and Data Responsibilization

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070-129 Lisbon
Portugal

Academic Editors
Ralf De Wolf (Ghent University, Belgium)
Mariek Vanden Abeele (Tilburg University, The Netherlands)

Available online at: www.cogitatiopress.com/mediaandcommunication

Table of Contents

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 158–162
DOI: 10.17645/mac.v8i4.3722

Editorial

Editorial: Children's Voices on Privacy Management and Data Responsibilization

Ralf De Wolf [1,]* and Mariek M. P. Vanden Abeele [2, 3]

[1] Department of Communication Sciences, imec-mict, Ghent University, 9000 Ghent, Belgium;
E-Mail: ralf.dewolf@ugent.be
[2] Department of Communication and Cognition, Tilburg University, 5000 Tilburg, The Netherlands;
E-Mail: m.m.p.vandenabeele@tilburguniversity.edu
[3] Department of Culture Studies, Tilburg University, 5000 Tilburg, The Netherlands

* Corresponding author

Submitted: 6 October 2020 | Published: 10 November 2020

Abstract
Contemporary children live in datafied societies in which they navigate and use technological innovations that drive on their personal information. Instructing privacy literacy is often presented as a key solution to help children manage their personal data responsibly. While there is agreement on the empowering potential of privacy literacy for children, there are also concerns over the burden that this responsibility places on them and their capacity for resilience. Children are key stakeholders in this debate. Nonetheless, we rarely hear their voices on issues related to their online privacy and data responsibilization. The articles included in this thematic issue account for this limitation by amplifying the voices of children, looking into the practices of parents and exploring the role of the tools being used.

Keywords
children; data responsibilization; empowerment; online; parents; privacy; sharenting

Issue
This editorial 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

Children spend substantial amounts of time in online environments (Demeulenaere, Boudry, Vanwynsberghe, & De Bonte, 2020). These environments offer children various opportunities to play, interact and develop their selves. However, because they also bring new risks, it is important to safeguard children's rights when interacting with them. In this context of protecting children's rights online, the notion of children's privacy has come under scrutiny. When children navigate and experience online environments, they leave behind personal information. It is often assumed that one needs to develop privacy literacy, which can be understood as a constellation of certain awarenesses, skills and attitudes that help them to manage their personal information responsibly (Trepte et al., 2015).

While there appears to be agreement on the empowering potential of privacy literacy for children, scholars have lately voiced their concerns over the burden that this responsibility places on audiences (De Wolf & Joye, 2019; Livingstone, 2019). Privacy literacy assumes that children themselves are capable of managing their own privacy online. Society, however, can also play a role in mitigating such data responsibilization. By pointing towards the responsibilities of service providers and other stakeholders, society might be able to provide some relief to children from the burden to be cognizant, literate and responsible for their personal information. While this new perspective suggests a balance between child empowerment and protection, it appears difficult to obtain in our contemporary neoliberal society.

Given that children are key stakeholders in the debate over their online privacy, it is surprising that we know little about their opinions, perceptions and experiences (Stoilova, Nandagiri, & Livingstone, 2019). This is unfortunate, as their stories may inform about the narratives that they learn and (re-)produce regarding the responsibilities of the different actors involved. These narratives, in turn, can inform about the social position of children in contemporary digital societies. The purpose of this special section is to amplify the voices of children with regard to privacy management and data responsabilization. The articles collected in this volume cover a broad spectrum of issues, topics, theoretical frameworks and methods that are oriented towards the lifeworld of children. Combined, the theoretical and empirical studies illustrate the complex interplay between children's practices, perceptions and opinions on the one hand and the conglomerate in which they find themselves on the other.

2. Amplifying the Voices of Children

The first four articles in this thematic issue amplify children's voices on privacy management and data responsibilization. Although privacy is generally considered as a basic human right (cf. Warren & Brandeis, 1890) enabling people to determine how and to what extent they disclose information to, and withdraw it from others (cf. Westin, 1967), research shows that privacy is experienced and felt differently depending on one's relative position within society (Marwick & boyd, 2018). If we truly want to hear the voices of children, it is therefore necessary to take into account their relative position within the household, in which they are often highly dependent on their parents or legal guardians. Such an analysis can inform about children's relative position in not only the household, but also in general society, and how that position shapes the meanings assigned to privacy and personal data, above and beyond children's cognitive abilities and individual skill sets.

Laurien Desimpelaere, Liselot Hudders, and Dieneke Van de Sompel (2020) present such an analysis in their article "Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study." Their article delves into the coping strategies and perceptions of children (aged 8–11) towards implicit and explicit forms of data collection for advertising purposes, interviewing both children and their parents. Although parents in their study express a certain level of knowledge with regard to data collection for advertising purposes and third-party usage, they mainly worry about 'stranger danger.' Children appear less cognizant about implicit data collection practices, but employ a variety of privacy coping strategies nonetheless (e.g., refraining from providing any personal details, or seeking parental guidance). Reproducing the perceptions and concerns of their parents, they formalized such strategies being mainly worried about malevolent parties. Desimpelaere et al. (2020) further demonstrate how parents and children care about privacy, but lack a full comprehension of various ways data are processed and used.

In "Strengthening Children's Privacy Literacy through Contextual Integrity" Priya Kumar, Mega Subramanian, Jessica Vitak, Tamara Clegg, and Marshini Chetty (2020) employ Nissembaum's contextual integrity framework to develop a new model of privacy literacy. Rather than focusing on factual or declarative ('knowing that') and procedural ('knowing how') knowledge, they instead "articulate privacy literacy as the practice of enacting appropriate information flows within sociotechnical systems" (p. 175). Drawing on interviews with 30 families (including 40 children), they validate their model by applying it to children's password management practices in an educational, family and friendship context. The results illustrate how password management practices differ between these contexts and how ascribing secrecy to passwords ("don't ever share your password with anyone") is not the most fitting transmission principle. Rather, passwords are shared with friends and family on the basis of trust. Kumar et al. (2020) therefore argue that—rather than merely memorizing and following rules that do not necessarily align with their practices—families need to "connect rules to norms and discuss rules in terms of contextually appropriate information flows" (p. 181) in order to allow children to grow, gain experience and develop privacy norms.

Using a context-sensitive ecological perspective, "Navigating Onlife Privacy: A Family Environment Perspective on Children's Moral Principles" by Joke Bauwens, Katleen Gabriels, and Lien Mostmans (2020) present findings of a focused ethnographic study with 10 socially privileged families in Flanders. Bauwens et al. (2020) treat the everyday family context as the primary realm of moral experience, in which children learn various principles to navigate 'onlife' privacy. They develop a theoretical lens that considers how individual, cultural and interpersonal moral values shape the process of concealing and revealing, and apply this lens in their inquiry of how families negotiate privacy. Based on participant observations and ethnographic interviews, the authors find that privacy is presented and established as a cornerstone of the household. While 'stranger danger' also informs the privacy practices of these families, Bauwens et al. (2020) found children to be morally motivated, as they "articulated a strong sense of co-responsibility in keeping their family safe" (p. 192). Interestingly, parents and children also expressed moral superiority when discussing the disclosing practices of other households.

In "Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy" Mariya Stoilova, Sonia Livingstone, and Rishita Nandagiri (2020) conducted group interviews with children and teens (age 11–16) to explore how they understand privacy in an interpersonal, institutional and commercial context. Using a contextual framework, the findings indicate that children employ many different privacy management strategies in interpersonal contexts and are familiar with the networked nature of the online environment. Even more significant, children first learn about interpersonal privacy and then "extend interpersonal assumptions to institutional and commercial contexts" (p. 200). However, they indicate how little agency and control they have in institutional and especially commercial contexts.

The above four articles are indicative of a paradigm shift in privacy research in the last two decades to not only focus on individual characteristics but also include interpersonal and contextual aspects of privacy (Bazarova & Masur, 2020; Nissenbaum, 2010; Stoilova et al., 2019; Trepte, 2020). This paradigm shift has now also made its way in privacy research on children. A question that remains, however, is how this shift can lead to a better protection of children's rights, as "neither a universalist approach centred on individual control nor a highly contextual approach to privacy is practical when it comes to protecting children's privacy in the current commercialized digital environment" (Stoilova et al., 2020, p. 198). In that context, a relevant observation that the above studies share is that children may show interest, but are not necessarily cognizant about commercial privacy. This means that parents have an important role in educating children and negotiating privacy norms. As the second set of articles in this thematic issue show, this parental mediation of privacy comes with its own challenges, as parental practices can generate risks for children's privacy.

3. Intimate Surveillance and Sharenting

While the rise of dataveillance (van Dijck, 2014) evokes widespread academic and public attention, lesser attention seems to go out to practices of surveillance in intimate relationships. In the context of children's privacy, the notion of intimate surveillance as coined by Leaver (2015) is especially valuable. Leaver defines intimate surveillance "as the purposeful and routinely well-intentioned surveillance of young people by parents, guardians, friends, and so forth" (Leaver, 2015, p. 153). Although caregivers often frame intimate surveillance as a care practice (Balmford, Hjorth, & Richardson, in press), the fifth and sixth articles in this thematic issue suggest its implications for child privacy can be profound.

First, in "'The Kids Hate It, but We Love It!'—Parents' Reviews of Circle," Davide Cino, Giovanna Mascheroni, and Ellen Wartella (2020) explore parental perceptions of intimate child surveillance by analyzing the discourse in 154 online reviews of the popular screen-time management and parental control device Circle. The reviews suggest that Circle users promote a restrictive form of parental mediation, by equating responsible parenting with controlling and monitoring your children. Paradoxically, while some parents describe Circle as a technology that temporarily reliefs them from the burden of 'intensive parenting' (cf. Lim, 2019), their use of the technology reproduces the very notion of the responsible parent as an ideal. As such, few reviews raised concerns about children's privacy, let alone critiqued the lack of children's agency.

Second, in "Privacy and Digital Data of Children with Disabilities: Scenes from Social Media Sharenting," Gerard Goggin and Katie Ellis (2020) argue that sharenting, a practice where parents share personal information about their children in social media, can be especially problematic in the context of the privacy of children with disabilities. Prior research shows that, overall, parents have the best interests of their children in mind when engaging in sharenting (e.g., showing that they are committed parents, or developing a digital family photo-album; Blum-Ross & Livingstone, 2017). However, the agency of children in this process is often limited (Ouvrein & Verswijfel, 2019). This is especially the case for people with disabilities, who often need to disclose personal information in exchange for obtaining care or receive accommodations. Paradoxically, "children with disability are rarely considered the owners of their private information. From their parents, to charity organizations to medical discourse writ large, the private lives of children with disability are considered public domain" (Goggin & Ellis, 2020, p. 221). Hence, personal information needs to be shared and is considered public. This observation perfectly illustrates how added layers of complexity further limit the agency of children with disabilities on top of general structural restraints of children. As the final article in this thematic issue shows, this issue cannot be solved simply by involving children in technology and privacy design.

4. Designing Technologies with and for Children

In "Designing Technologies with and for Youth: Traps of Privacy by Design," Bieke Zaman (2020) argues that involving children in privacy design is an important step towards protecting their rights. In her critical sociotechnical reflection of the field, she identifies three traps to participatory design research with children: relying on guidelines that assign limited decision power to children, approaching children as consumers rather than citizens, and creating conditions that are actually superficial or misleading rather than empowering. These traps have profound implications for privacy-by-design efforts, and require a design agenda that rethinks traditional notions of participatory design. This agenda, Zaman (2020) argues, should move beyond making the 'right' design choices to mitigate risk or harm by also addressing the unique experiences and meaning-making processes of children living in a data-driven society.

Together, the seven articles in this thematic issue highlight the importance of adopting a holistic and contextual perspective, as it is impossible to discuss children's privacy without acknowledging the role and the practices of parents and other persons in their lives, as well as the broader context of a datafied culture in which attention is commodified. As such, we hope that this thematic issue takes the debate on children's privacy and data responsibilization one step further. On a final note, we would like to highlight how the empirical studies included in this thematic issue mainly focus on privacy and data responsibilization with regard to social media and smartphones. The emergence of The Internet of Things (IoT) further enables interconnections between people and objects, also leading to ambient and ubiquitous devices within households. Smart speakers, thermostats, personal assistants, cameras, and other such technologies permeate Western households and are becoming a central feature of the 'networked family.' Evidently, always-listening or always-watching speakers, screens and cameras raise significant privacy challenges on multiple fronts for all household members, including children. Indeed, much remains to be investigated to further understand privacy among children, stimulate empowerment and mitigate responsibilization.

Conflict of Interests

The authors declare no conflict of interests.

References

Balmford, W., Hjorth, L., & Richardson, I. (in press). Supervised play: Intimate surveillance and children's mobile media usage. In L. Green, D. Holloway, K. Stevenson, T. Leaver, & L. Haddon (Eds.), *The Routledge companion to digital media and children*. New York, NY: Routledge.

Bauwens, J., Gabriels, K., & Mostmans, L. (2020). Navigating onlife privacy: A family environment perspective on children's moral principles. *Media and Communication*, *8*(4), 185–196.

Bazarova, N., & Masur, P. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118–123.

Blum-Ross, A., & Livingstone, S. (2017). "Sharenting," parent blogging, and the boundaries of the digital self. *Popular Communication*, *15*(2), 110–125.

Cino, D., Mascheroni, G., & Wartella, E. (2020). "The kids hate it, but we love it!": A content analysis of parents' reviews of Circle. *Media and Communication*, *8*(4), 208–217.

Demeulenaere, A., Boudry, E., Vanwynsberghe, H., & De Bonte, W. (2020). *Onderzoeksrapport: De digitale leefwereld van kinderen* [Research report: The digital lifeworld of children]. Gent: Mediaraven.

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Children's and parents' perceptions of online commercial data practices: A qualitative study. *Media and Communication*, *8*(4), 163–174.

De Wolf, R., & Joye, S. (2019). "Control responsibility": A critical discourse analysis of Flemish newspapers on privacy, teens and Facebook. *International Journal of Communication*, *13*, 5505—5524.

Goggin, G., & Ellis, K. (2020). Privacy and digital data of children with disabilities: Scenes form social media sharenting. *Media and Communication*, *8*(4), 218–228.

Kumar, P., Subramanian, M., Vitak, J., Clegg, T., & Chetty, M. (2020). Strengthening children's privacy literacy through contextual integrity. *Media and Communication*, *8*(4), 175–184.

Leaver, T. (2015). Born digital? Presence, privacy, and intimate surveillance. In H. John & W. Qu (Eds.), *Re-orientation: Translingual transcultural transmedia—Studies in narrative, language, identity, and knowledge* (pp. 149–160). Shanghai: Fudan University Press.

Lim, S. S. (2019). *Transcendent parenting: Raising children in the digital age*. New York, NY: Oxford University Press.

Livingstone, S. (2019). Audiences in an age of datafication: Critical questions for media research. *Television and New Media*, *20*(2), 170–183.

Marwick, A., & boyd, d. (2018). Privacy at the margins: Introduction. *International Journal of Communication*, *12*, 1157–1165.

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

Ouvrein, G., & Verswijfel, K. (2019). Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management. *Children and Youth Services Review*, *99*, 319–327.

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, *8*(4), 197–207.

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

Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, *2020*. https://doi.org/10.1093/ct/qtz035

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). Heidelberg: Springer. https://doi.org/10.1007/978-94-017-9385-8

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*, 197–208.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Zaman, B. (2020). Designing technologies with and for youth: Traps of privacy by design. *Media and Communication*, *8*(4), 229–238.

About the Authors

Ralf De Wolf (PhD) is a Postdoctoral Researcher and Assistant at the Department of Communication Sciences and connected to the research group for Media, Innovation and Communication Technologies (imec-mict-UGent), Ghent University, Belgium. His current research and interests focus on the privacy management of children and teens, automation, algorithms and inequality. Ralf's work is published in leading journals in the field, such as *New Media & Society* and *International Journal of Communication*.

Mariek M. P. Vanden Abeele (PhD) is Associate Professor in Digital Culture at Tilburg University. Mariek combines media psychological and media sociological perspectives to understand how digital media affect life and society. Her interests include mobile communication and social relationships, problematic smartphone use and digital wellbeing, mobile media and childhood, and the implications of self-tracking for health. Mariek's work is published in leading journals in the field, such as *New Media & Society* and *Media Psychology*.

COGITATIO

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 163–174
DOI: 10.17645/mac.v8i4.3232

Article

Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study

Laurien Desimpelaere [1,*], Liselot Hudders [1,2] and Dieneke Van de Sompel [1,2]

[1] Department of Communication Sciences, Faculty of Political and Social Sciences, Ghent University, 9000 Ghent, Belgium; E-Mails: laurien.desimpelaere@ugent.be (L.D.), liselot.hudders@ugent.be (L.H.), dieneke.vandesompel@ugent.be (D.V.d.S.)
[2] Department of Marketing, Innovation and Organization, Faculty of Economics and Business Administration, Ghent University, 9000 Ghent, Belgium

* Corresponding author

Submitted: 6 May 2020 | Accepted: 13 July 2020 | Published: 10 November 2020

Abstract
Children's personal data are often collected for commercial aims. Although regulations in different countries aim to protect children's privacy (e.g., by imposing websites to request parental consent for the processing of children's data for commercial purposes), concerns about protecting children's online data continue to rise. This article therefore aims to get insights into parents' and children's privacy coping strategies and perceptions underlying these strategies. In-depth interviews with ten parents and nine children (8–11 years) were conducted. Findings show that although children engaged in avoidance (e.g., leaving the particular website) and confrontation (e.g., seeking support) strategies, they mainly did this to protect their privacy from malicious individuals—and not from commercial parties. Participating children also lacked general knowledge about both explicit and implicit data practices. To protect their children's privacy, parents in this study mainly adopted restrictive mediation strategies, but lacked the knowledge to undertake concrete actions in the case of implicit data collection. Implications for policymakers are discussed.

Keywords
children; coping; data collection; online privacy; parents; privacy literacy

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

The development of digital technologies and children's heavy internet use has facilitated the collection of children's personal data for commercial aims, such as personalised services and advertisements. This has led to regulations to protect children in this matter. Regulations such as the Children's Online Privacy Protection Act in the United States and the General Data Protection Regulation in Europe impose certain requirements on websites regarding data collection when targeting children under 13 and 16 years of age. Websites are, for instance, required to obtain verifiable parental consent for collecting and processing children's online data (Lievens & Verdoodt, 2018).

Parents have thus been given a crucial legal responsibility in their children's online data management, and can fulfil this role by, for instance, applying safety measures. One study, for instance, found that children who had indicated that their parents impose certain restrictions on what they could watch on YouTube, had better online safety beliefs (e.g., the degree to which they, for instance, believed that their online data goes away when leaving the internet (Andrews, Walker, & Kees, 2020). Despite this important parental role, academic research has rarely examined parents' view on online commercial data collection practices, and whether and how they take up this responsibility. The limited research on general privacy issues suggests that parents are concerned about the information collected from their kids (Anderson, 2019), yet often feel unsure about addressing general online safety issues (Third, Spry, & Locke, 2013). A lack of data protection knowledge is, however, commonly associated with the inability to effectively regulate one's online privacy (Trepte et al., 2015). This may thus imply that parents are potentially unable to optimally manage their own online privacy, which subsequently questions their ability to take on a role as caretaker of their children's online privacy. In this perspective, it might also be interesting to explore whether children themselves have insights on how they can manage their own online privacy. Although previous studies (Park, 2013; Park, Campbell, & Kwak, 2012; Youn, 2009) showed that people can engage in a range of privacy protective measures which they deem appropriate to safeguard their privacy and data (e.g., closing the website, giving fake data), little research actually explored how children and parents use these strategies to cope with online data requests from commercial entities.

Based on in-depth interviews, this article provides a first insight into parents' and children's (8–11 years) perceptions of the collection and use of their data for advertising aims and the strategies they use to protect their online privacy. Insights in this topic are urgent for educators and policymakers that aim to protect children's privacy. This study also extends findings from previous research by elucidating how parents and children perceive their online privacy in today's digital ecosystem, and how such perceptions affect their strategies to cope with attempts to retrieve their online data.

2. Related Work

2.1. Different Types of Commercial Data Collection

Today's variety of digital media has facilitated advertisers to gather people's data online. The ways in which this data can be commercially employed seem to be endless: from using it to refine marketing campaigns by creating advertising messages that are more likely to be of users' interest, to improving customer experiences in such ways that products and services meet consumers' demands, and to selling large amounts of data to businesses to make a profit from it, among others.

The extraction of data can generally be distinguished into two different approaches, namely explicit and implicit data collection (Taylor, Davis, & Jillapalli, 2009). Personal data can be explicitly collected when users provide their data entirely voluntarily. Such data includes demographic data, profile information and pictures, and can be collected from, among others, registration forms or single sign-on applications. Alternatively, commercial entities can also implicitly collect data by, for instance, tracking users' geolocations by means of cookies. These cookies are small text files stored on computers' hard disks and gather data about internet users' online browsing behaviour, such as preferred language and contents of shopping carts. This study incorporates both types of commercial data collection. More specifically, the study examines how parents and children perceive these practices and how they cope with these specific types of data requests.

2.2. Strategies to Cope with Data Collection

When data collection is initiated, people need to decide on whether they want to share information or adopt protective measures. These decisions are both components of privacy management. When people decide to go for the latter, they can choose from two different privacy management strategies, namely avoidance and confrontation (or approach) strategies (Smit, van Noort, & Voorveld, 2014).

Coping by avoidance concerns actions to refrain websites from collecting one's data. Examples are categorised by previous studies as refrain strategies (Youn, 2009) whereby users stop visiting the particular website that requests personal data or go to other websites that do not request these details. In other words, users will refuse to provide personal information. Besides, refusing the installation of cookies, and rectifying strategies, such as asking the website to remove personal data (Park et al., 2012), may also be labelled as avoidance strategies.

Coping by confrontation (or approach) is characterised by users' active role to better understand the mechanisms of data practices and to defend themselves against it, often described as all skills related to 'mastering the internet' (Smit et al., 2014). It specifically refers to functional strategies such as information- or advice-seeking (e.g., asking others for guidance and reading privacy statements), fabricating or providing incomplete personal information (Youn, 2009), and installing technological protective measures (e.g., filters to block unwanted emails, removing cookies, software that conceals the computer's identity from visited sites; Park et al., 2012).

2.3. Children's Privacy Perceptions

When it comes to children, we assume perceptions of privacy and personal data is subject to age due to developmental and cognitive differences. The developmental process through which children go is related to their cognitive maturation and entails acquiring various skills concerning cognitive resources and theory of mind, or the recognition that what is in their mind may differ from that what is in other people's minds (Perner & Lang, 1999). Prior work exploring children's and teenagers' privacy perceptions and management indeed suggests differences between younger and older age groups. For instance, Feng and Xie (2014) found that children are less concerned about their data being collected by marketers than their parents are. Moreover, Turow and Nir (2000) found that children between 10 and 17 years old were much more likely to provide sensitive personal data to commercial sites in exchange for a free gift than their parents. In the context of social network sites, teenagers also reported employing fewer privacy settings than adults (Christofides, Muise, & Desmarais, 2012).

It is not that children do not care about their online privacy—they are able to identify privacy risks such as oversharing, but they often struggle to completely understand other threats, such as online tracking (Zhao et al., 2019). In one survey with an open-ended question, European 9 to 16-year-olds articulated a variety of privacy risks they encounter on the internet (Livingstone, Kirwil, Ponte, & Staksrud, 2014). Most of the expressed concerns were related to risks regarding content that is of a sexual or violent nature, and less attention was devoted to privacy threats related to online tracking practices. Furthermore, in the study of Brooks and Moeller (2019), children (9–11 years old) were not aware of all risks associated with information disclosure as they mostly related the concept of privacy with strangers misemploying their personal data. In another study, most children of 5–11 years old did not see adequate privacy management as the implementation of additional privacy measures (like providing false information), but, instead, mainly relied on their parents' support to manage privacy online (Kumar et al., 2017).

2.4. Parental Mediation Strategies to Protect Children's Online Privacy

Parents can thus step in to protect their children from exposure to online risks. They are generally seen as the primary socialisation agents in teaching children the complexities of the media environment (Shin, 2015). According to the parental mediation theory (Clark, 2011), parents' efforts to mediate harmful effects of media on children are typically distinguished in restrictive and instructive mediation strategies. Similar to the avoidance strategy, parents may protect their children restrictively by setting limitations to avoid undesirable aspects of children's internet consumption, such as forbidding children to disclose information or to agree with cookie notices. Similar to the confrontation coping strategy, parents may adopt an instructive mediation strategy by enhancing an open dialogue with their children and educating them about privacy management (Hudders & Cauberghe, 2018). Instructive forms of parental mediation strategies are considered to be more effective than restrictive forms, and have indeed been found to be more effective in reducing information disclosure among adolescents (Shin & Kang, 2016). Such a mediation strategy is after all based on a critical discussion between parent and child, and it is more likely to encourage children to develop their critical thinking skills. Previous work also showed that parents favour social mediation (e.g., restrictive and instructive mediation) over system-based regulation, such as installing technical software (Kirwil, 2009). The study of Livingstone and Helsper (2008) found that parents implement on average about eight different types of mediation to regulate their teenagers' online presence, ranging from talking about internet use, setting maximum screening times, and forbidding children to do online shopping. In reality, it thus seems that parents often use a variety of strategies to shield their kids' privacy.

2.5. The Importance of Privacy Literacy for Engagement in Privacy Protective Behavior

The literature often looks at disclosure behaviour through the lens of the privacy calculus theory, which assumes that users employ a cost-benefit trade-off prior to deciding on accepting or rejecting data requests, and that they will only disclose personal information when the benefits exceed the expected (privacy) losses (Kokolakis, 2017). Typical benefits entail access to certain content, monetary incentives, personalised advertisements, and customisation benefits (Babula, Mrzygłód, & Poszewiecki, 2017; Li, 2012). Risks include negative consequences of online disclosure, such as risks of privacy invasion (Li, Sarathy, & Xu, 2010), privacy loss due to organisational misuse and lack of data protection (Xu, Dinev, Smith, & Hart, 2011), unauthorised use of personal data by third parties and nuisance from unwanted advertisements (Prince, 2018).

Being literate is however a stipulation for being able to make these cost-benefit trade-offs. Media literacy that covers different types of literacy, such as privacy and advertising literacy, encompasses a variety of skills that people need to have to be able to critically analyse messages in audio, print, video, and multimedia (Hobbs, 1999) and has been put forward by scholars as an empowering element in engaged citizenship (Mihailidis & Thevenin, 2013). The acquirement of such literacy enables individuals to make rational decisions and have the cognitive tools to interact with all types of media, both online and offline (Masterman, 2003). Having overall knowledge and insights into the business models that companies use may also raise awareness about privacy harms and is necessary for individuals to make evaluations and consolidated decisions on disclosure (Trepte et al., 2015). That is, knowing that a company will use personal data for commercial purposes may evoke engagement in privacy protective behaviour. This may be problematic when it comes to children because they have different levels of developmental and cognitive capabilities than adults have and may thus not possess such know-how and data protection abilities. For instance, in the context of advertising, it was found that at the age of 12, children have still not developed an adult-like understanding of advertisers' selling and persuasion intentions (Rozendaal, Buijzen, & Valkenburg, 2010). Also, they sometimes overvalue their understanding of marketing practices and, as a result, eventually engage in more risky behaviours (Shin, Huh, & Faber, 2012). Beside their underdeveloped privacy literacy, their cognitive control is not yet entirely matured and may even get surpassed by affective reward processes too. This may make them biased toward appraising the benefits that are given in return for data, and may lead to greater willingness to disclose data and smaller motivation to protect their privacy (Walrave & Heirman, 2013; Youn, 2009).

3. This Study

This study adds to the current literature by proposing two research questions. First, the study explores if and how parents and children cope with both explicit and implicit data collection practices, and if and how parents undertake additional protective measures to protect their children's online privacy. Second, the study assesses the role of privacy literacy and perceptions of these practices on parents' and children's decisions to engage in protection strategies or to go along in the request to provide data.

4. Method

4.1. Study Design

In-depth interviews with parents and children from the same family (separately interviewed) were conducted (all by one researcher). The interviews with the children lasted between 20 and 45 minutes approximately, and those with the parents took between 35 and 50 minutes. All interviews were run by the same researcher in a classroom of one Flemish Belgian primary school (except for two that took place at home and at the work of the concerned parent respectively, due to logistic reasons). All interviews were conducted in January 2018. Ethical approval was obtained from the researchers' university, and written consent was received from the concerned primary school, parents and children.

4.2. Participants

Nine children (*M* = 9.9; *SD* = 1.17), seven boys and two girls, and ten parents between 36 and 49 years old (*M* = 41.7; *SD* = 3.66), eight women and two men, partook in the study (see Table 1). Children between 8–11 years were selected because of the following reasons. First, a certain level of internet usage was required to make sure that children have already been confronted with explicit data requests. About 94% of children between 8 and 11 years old use the internet (Ofcom, 2017). Characterised by the analytical stage of consumer socialisation, it is also from this age onwards that children develop a more complex theory of mind and a more sophisticated understanding of the complexity of the marketplace (John, 1999). They develop skills to assess the appropriateness of data practices, and they are able to grasp complicated concepts such as online privacy (Kumar et al., 2017). Children are then at least cognitively able to understand this study's theme, and in turn, it makes the topic more addressable in the interviews.

4.3. Procedure and Interview Guide

The in-depth interviews consisted of three parts: (1) An introduction in which the research objective was explained and anonymity was guaranteed, followed by questions about coping with (2) explicit data practices (website subscriptions and contest participation) and (3) implicit data practices (existence of cookies and personalised ads). For these two parts, children were shown a video including a scenario in which a child is faced with website subscription, as well as a screenshot of a

Table 1. Participants' demographic information.

Parent			Child		
Name	Gender	Age	Name	Gender	Age
Abigail	F	41	Liam Benjamin	M M	11 8
Alexx	F	43	Samuel	M	11
Aaron	M	41	Mario	M	9
Sophie	F	36	Edward	M	9
Oliver	M	41	Olivia	F	9
Ilse	F	41	Tommy	M	10
Anna	F	49	Devlin	M	11
Nancy	F	44	Sara	F	11
Gabriela	F	41			
Eva	F	40			

Note: Fictive names are used to guarantee anonymity.

cookie consent banner on a website. Afterwards, questions were asked regarding their recognition of, and previous experiences with, both practices and their understanding of (the business model underlying) these practices (e.g., ‘Why would a company be interested in your information?’). Parents were asked similar questions but were instead shown several screenshots of (child) websites requesting to fill in profile data.

Children then watched another video explaining (in a child-friendly way) what cookies and personalised advertisements are, and completed questions about their affective reactions (e.g., ‘What do you [dis]like about it?’). Parents were asked similar questions after they were verbally explained what cookies and personalised advertisements are, and were shown examples of personalised advertisements. Next, a sorting task was performed to identify whether respondents use privacy protective strategies. They needed to allocate different kinds of personal data (e.g., home address, favourite colour) to a pile representing the extent to which they would (allow their children to) disclose that piece of information, and were asked what they do when they are confronted with cookie notices. Parents were also inquired whether they took additional measures to shelter their children’s privacy (e.g., implementing ad blockers, deleting cookies, imposing restrictions on revealing information). See Appendix I (in the Supplementary File) for materials used during the interviews.

4.4. Data Analysis

The data was analysed making use of the model of Miles and Huberman (1994), consisting of several steps, namely data collection, data reduction (selecting, simplifying and coding data extracts), data display (structuring the data) and drawing conclusions. More specifically, when all in-depth interviews were conducted, they first were transcribed and screened on relevant data extracts, using the open source RQDA for qualitative data analysis. These data extracts were then labelled by initial codes (i.e., short descriptions) that reflected the meaning of the extract (e.g., ‘lies about personal details’). Next, we structured all descriptions into specific themes so that they matched the research questions: (1) coping strategies; and (2) privacy literacy and perceptions (see Appendix II, in the Supplementary File, for the used codes). The process of screening the interviews on relevant data extracts, assigning codes and allocating these codes to the selected themes was reiterated multiple times to ensure all relevant data extracts were coded. The already-allocated data extracts were then reviewed to assure a consistent match between the codes and the themes so conclusions could be drawn. Only power quotes (most representative ones for the category) are included in the results section. Additional quotes supporting the prevalence of our findings are included in Appendix II (proof quotes, in the Supplementary File; Pratt, 2008).

5. Results

5.1. Children’s Coping Strategies

Results show that children often respond favourably to companies’ explicit and implicit data requests and are willing to provide some details to a certain degree. For instance, all children would give details such as first name, gender, city, favourite colour, and TV show when companies request them, while three kids would also accept cookie consent banners themselves (without asking their parents’ permission).

Children in this study also undertake protective measures (avoidance as well as confrontation strategies) to cope with data practices. One child mentioned he would move away from a website that requests personal details—an example of an avoidance strategy, ‘I would look for another game [when the game requests personal details]’ (Benjamin, 8). Another avoidance strategy was to click away cookie banners, ‘So if my finger is the computer mouse, then you can click outside it and then it goes away’ (Devlin, 11). Alternatively, examples of confrontation strategies included lying about personal details, ‘I would give a wrong street and number, like Flower District 78’ (Samuel, 11), and seeking support by asking parents for guidance in the decision to accept the cookie consent banner, ‘If mom has read it, then I would agree and if she’s not there, I am not allowed to, so I don’t’ (Edward, 9).

5.2. Children’s Privacy Literacy and Perceptions of Data Practices

The study reveals a number of elements that may explain children’s coping decisions.

5.2.1. Incomplete Understanding of How Data Collection Practices Work

None of the interviewed children could correctly reveal the reasons why companies would be interested in personal data. Instead, six of them allocated companies’ interests in personal data to a dishonest agenda, ‘They might pass on your information to crooks and when they have bad intentions, they will rob you’ (Liam, 11).

Results also indicated that children have not a full understanding of how data collection practices work. More specifically, six children had no idea what cookies are and for what purposes they are installed on users’ computers. The other three children wrongly guessed a cookie was ‘a virus’ (Benjamin, 8), ‘a strange ad’ (Mario, 9), or a notice that ‘they are changing the website’ (Sara, 11).

5.2.2. Some Level of Privacy Consciousness

Although children may not spontaneously understand the consequences of data practices for their online privacy, they did seem to hold a certain level of privacy consciousness. For instance, six children discussed explicit data disclosure in terms of potential data abuse by dishonest parties, ‘I’m not going to give my address or phone number, because when a thief would ask your address, they can break into your house’ (Mario, 9). To this end, they were also less willing to provide personally identifiable data (e.g., home address or phone number) as they associated it with potentially severe misuse, ‘I think that websites with not so good intentions cannot do anything wrong with these data [points at non-identifiable data], but they can with this data [points at identifiable data]’ (Sara, 11). In this regard, they disclosed personal details only when they perceived the website trustworthy, ‘I would fill that in because it’s VTM [Flemish television channel], so what would they do with that? That’s okay for me’ (Devlin, 11). Besides, some children seemed to have a primary understanding of privacy in the context of websites’ cookie practices too. For instance, once children were explained how cookies work and saw an example of a targeted ad, four children evaluated these ads as ‘weird’ or ‘annoying’ because ‘you don’t expect something standing over there that you looked for a few days ago’ (Samuel, 11). Three of the interviewed kids even implicitly referred to their online privacy and private space, and did not like the idea of being tracked by cookies, ‘That’s actually a bit intruding in people’s private life, and I don’t like that’ (Samuel, 11).

5.2.3. Positive Attitude toward Use of Personal Data

Despite having some concerns, children were largely positive about data collection practices. They valued the idea of getting emails about products they like ‘because then you know that there is a reduction’ (Sara, 11), and appreciated the fact that website registration (and thus having a profile) enables participation and access to content visitors do not have. Edward (9) also explained he was happy receiving rewards in turn for his personal data, ‘I was playing a game, and suddenly I needed to log in….So I logged in, which wasn’t that bad at all, and then I got some stuff [game rewards].’ Additionally, when children were asked whether they would provide sensitive data in exchange for an imaginary gift, four of them would undoubtedly do so, sometimes even ‘no matter what the gift is’ (Devlin, 11). Moreover, in the context of implicit data practices, Sara (11) concentrated on the relevance of online behavioural advertising, ‘It [the advertised product] might be more fun than other products you saw in the shop,’ and Benjamin (8) liked the idea that advertisements about interesting products would “follow” him in case he would not be able to find the products himself.

5.3. Parents’ Coping Strategies

Many parents did not use protective strategies for their own data, ‘You just provide your details quite quickly, don’t you? I don’t really dwell on it, you just do it, because it is required’ (Ilse, 41). Six parents also accepted cookie notices ‘to be able to continue’ (Abigail, 40) or because they ‘didn’t know what it exactly was’ (Eva, 40). Only a handful of interviewees adopted protective measures, in the form of avoidance strategies, to shield their personal data, and this was only when companies explicitly requested personal data. They for instance used multiple accounts, ‘I have a special email address for spam things’ (Aaron, 41), and withdrew from providing information. Oliver (41) saw unsubscribing (a rectification strategy), as the solution to optimally gain from the benefits of registration, yet, not to be overwhelmed by the flow of newsletters.

While the parents in this study undertook few measures to protect their own personal data, they did want to have control over their children’s privacy. They for instance disallowed their children to subscribe, ‘I wouldn’t let him subscribe, because I think he needs to keep a form of privacy’ (Aaron, 41), incited them to ‘search for another game website where you don’t need to fill in your data’ (Eva, 40), or completed subscription forms themselves, ‘I’ll always fill in my child’s data myself’ (Gabriela, 41). In other words, by imposing certain rules, they mostly adopted restrictive mediation strategies to protect their children’s data. Further, Abigail (41) tried to initiate dialogue with her eldest children by explaining how to subscribe and support them whenever needed—a clear example of an instructive mediation strategy, ‘From the moment they were 14, we subscribed together. We really try to explain it, and whenever they have questions about it, they know they can ask us.’ She also explained the side effects of irresponsible data provision with her son when he provided his address to a complete stranger on the internet. It thus seems that parents might use both restrictive and instructive mediation strategies—and this in the function of previous privacy invasion experiences and the child’s abilities and age.

It is remarkable that while parents adopted some protective measures for explicit data requests, they did not do so in the case of implicitly collected data. Three parents knew cookies could be erased, yet, they found it an uncomfortable and annoying solution because of the hassle of looking up and giving in the previously saved information, such as logins and passwords, again after the deletion, or did not systematically reject cookie notices because they find it more convenient ‘to quickly continue’ (Abigail, 41). One parent rejected accepting cookie notices, yet, she seemed to handle it based on ignorance, ‘And what do you mean with cookies? Every time they ask me “Will you accept cookies?,” I don’t accept them’ (Gabriela, 41). Moreover, Sophie (36) who initially found personalised ads as ‘manipulative,’ perceived it too ‘complicated’ to actually install ad blockers. Confrontation strategies in the form of technological privacy control measures (e.g., erasing cookies, using ad blockers) were thus less often used.

5.4. Parents' Privacy Literacy and Perceptions of Data Practices

5.4.1. Incomplete Understanding of How Data Collection Practices Work

All parents in this study understood well that explicitly collected data is part of a profit-making business—they related it with advertising purposes and third-party use. However, in the context of implicit data practices, they showed a rather underdeveloped understanding of how personal data could be collected and used. Cookies were, for instance, referred to as 'cache data' (Ilse, 41) and were additionally wrongly assigned to a computer's working speed, 'If the computer is working too slow, I clean all those cookies and history' (Alexx, 43). While parents spontaneously mentioned occasions in which they were confronted with online behavioural targeting, two were initially unaware of how these advertisements are created, among Nancy (44):

> If you look up something on a website, then the next time you go online, there are ads everywhere. For instance, when you book a trip, then suddenly: trips, trips everywhere. There must be something linking everything. I don't know.

5.4.2. Concerns about Children's Personal Data

When it comes to their kids' personal details, many concerns were expressed. Sophie (36) and Anna (49) both felt revulsion toward advertisements based on their children's personal data, and especially doubt whether young kids are able to form critical attitudes towards these ads, as Anna (49) explained, '*I* know what *I* looked up on the internet, and *I* am able to let loose of these ads….But that's the hard part, especially for kids.'

Yet, most of the concerns were expressed in the area of stranger danger situations. Gabriela (41), for instance, worried substantially more about the potential misuse of their children's data by malevolent parties and the consequences related to this abuse, rather than about the use of their personal data for advertising aims: 'Okay, marketing….I understand those people, they want to make children consumer-minded. But paedophiles have it too [children's data]….I'm not afraid about this [data used for advertisements], I'm afraid about bad people using it to attack our children' (Gabriela, 41).

Also Alexx (43) expressed her worries regarding malicious individuals, and spontaneously told about the situation in which she was shocked to find out one of the followers of her eldest son's Instagram profile posted nude pictures of children. However, moments later, she did not care too much having her children being subscribed to some commercial websites, 'If you share your details on the internet, you need to take the consequences too.' This was also acknowledged by her son Mario (9) who indicated she is somewhat careless when it comes to her own privacy, 'She was looking for a new bike and she agreed [with the cookie notice], and she didn't even read it…and then the next day I watched YouTube on her phone and I saw advertisements [of these bicycles].'

Ilse (41) had neither yet experienced any form of privacy invasion so far and did not worry about the consequences of data practices, 'I've never really worried about it because we didn't have any problems with it so far. We actually don't need these ads, but I think we [she and her boys] are strong enough to resist them.' Hence, like Gabriela and Alexx, she did not perceive the privacy losses concerning data practices to be very high. This may also clarify why some parents are less interested in undertaking privacy protective strategies for the safeguard of their children's privacy, and why children in the first place engage in strategies to protect their privacy from malicious individuals, rather than from advertising purposes (see Section 5.2.2).

5.4.3. Mainly Negative Attitude toward Use of Personal Data

Parents evaluated companies' use of their online behavioural data mainly negatively. For instance, Alexx (43) explained she was irritated by the enormous amount of advertising mails in her mailbox:

> If I see something like 'This seems nice,' before I actually realize 'I shouldn't do this,' it [personal data] is already gone. And then, you see those emails entering your mailbox. Last week I suddenly had 500 emails, that's very annoying.

Besides, they believed their personal space was not always respected, and referred to manipulation and unconscious persuasion: 'I have problems with things that are pushed….This is brainwashing, because you look at this [the website content], but from the corner of your eye you only see this [the ad]. This is a form of manipulation' (Sophie, 36).

Some of them were even more sceptical about personalised advertising targeted at children. Ilse (41) opined that this form of advertising should not be allowed because of its recurrent and personalised character, 'It [the product] is stuck in their head for a longer period, and they won't forget it that easily.'

5.4.4. Perceived Lack of Control and Complacency

Some parents believed privacy protection to be out of their control, especially in the case of implicit data practices. This is demonstrated by five parents, including Gabriela (41): 'What can we do about it? I don't know. If I could, I'd love to protect my child but we don't have any control.' She allocated this lack of control to the ability of businesses to track down individuals' actions anytime users go online, 'Because, once you step on the internet, what you are searching, what you are doing….It's somewhere memorised. It's something that they can always check' (Gabriela, 41). Moreover, while some parents knew cookies could be erased, they did not always act upon this. Put differently, together with the fact that they are insufficiently informed about effective privacy protective strategies and show a low perceived self-efficacy, they also find it too effortful to actually take appropriate actions.

6. Conclusion

6.1. Discussion

This article not only investigated to what extent parents take on their legal responsibility to protect their children's online privacy, but also how children cope with online data practices. Several conclusions can be derived from this study.

In line with previous studies' finding that children struggle to completely understand online privacy threats (Kumar et al., 2017), children in this study lacked sufficient knowledge about both explicit and implicit commercial data practices and its underlying mechanisms (how data is collected, and for what it is used). Moreover, while some of the interviewed children did have some privacy awareness when they were prompted so, they generally seemed to put a greater emphasis on the benefits of e-marketers' data practices than on possible privacy infringements. They praised these practices for a better user experience, rewards, and ad relevance. Thus, the gains that come with sharing personal information outweigh the perceived risks, a finding that Boyd and Marwick (2011) also found among teenagers in the context of social network sites. The combination of a lack of knowledge and the rewards that are provided by institutions to entice users to share data may, unfortunately, result in children being prone to unconscious data sharing. However, privacy literacy and, by extension, media literacy is a premise for active citizenship: without this knowledge, users are only passive consumers of (online) information and communication (Livingstone, 2004).

The interviewed children also allocated motives for e-marketers to gather data to dishonest parties and were mainly worried about data abuse by malevolent parties. With respect to their coping strategies, some of them were willing to disclose certain information without engaging in protective actions. Children who did try to safeguard their online identity reported a variety of protective measures, including both avoidance strategies, such as refraining from providing information, and confrontation strategies, such as fabricating information and seeking parental guidance. Yet, these children did so only when they perceived the website to be untrustworthy or when they feared potential unfair data exploitations by malicious parties ('thieves'). A potential explanation for this may be found in the research of Young and Quan-Haase (2013) who found that undergraduate students have developed a number of privacy protective strategies in function of their privacy needs. More specifically, they felt a greater urge to engage in privacy protective strategies in the case of social privacy threats than when institutional privacy risks occurred. Participants simply did not raise many concerns about the use of personal data used by commercial institutions, but did engage in actions (e.g., shielding profile information for unwanted audiences on social network sites) in an attempt to protect their social privacy. The different needs related to social and institutional privacy may be one reason why children in this study adopted privacy protective strategies in one situation but not in another: It might be that children only have been told to be conscious with providing personal data in some online activities (e.g., chatting with strangers), but not in others (e.g., subscribing to commercial websites).

Parents in this study understood that personal information is commercially meaningful for businesses. Some of them therefore undertook privacy protective measures in the form of avoidance strategies (e.g., unsubscribing). They nevertheless seemed to lack this competence in the case of implicit data practices. They for instance perceived online behavioural targeted advertising as manipulative, yet, they often lacked knowledge about effective coping strategies, perceived it to be out of their control or found it too burdensome to undertake protective measures accordingly. This finding is in line with the study of Hanus and Wu (2016) who put forward that response-efficacy and self-efficacy are significant predictors of reported security behaviour. Not knowing how to implement effective privacy control measures and not being confident in one's ability to protect data accordingly ('What can we do about it?') may be the ground for irresponsible privacy behaviour. This finding is also a demonstration of the privacy paradox (Kokolakis, 2017): although parents in this study label data practices as an infringement to their privacy, this concern is not reflected in their behaviour as they do not take (too much) measures to protect their own and their kids' online information. In this context, it is also relevant to mention the concept of privacy cynicism (Hoffmann, Lutz, & Ranzini, 2016). This concept refers to the cognitive coping strategy that users appropriate in which they feel uncertain, mistrusted, and powerless towards e-marketers' data practices and whereby they rationalise privacy protective measures as completely useless or ineffective. Indeed, some parents in this study emphasised multiple times that commercial data practices belong to today's online environment and thought it is hard to effectively counteract the negative effects of it by implementing privacy protective measures.

When it comes to protecting their kids' privacy, the interviewed parents mainly engaged in restrictive mediation strategies (e.g., imposing them to use a website that does not request personal data), and again, did mainly so in the case of explicit data practices. Some parents also engaged in instructive mediation strategies (e.g., explicitly explaining the potential threats to their children) when their kids seem to be ready in terms of age and internet abilities. A possible explanation for the principal use of restrictive mediation strategies can be found in Lee's study (2013). His study found that the younger the child is, the more often parents use diverse restrictive strategies. This may be because young children have still not fully developed skills to cope properly with online risks independently and therefore mainly benefit from external guidance and restrictions.

Furthermore, some interviewed parents elaborated on their concerns with respect to their kids' internet privacy. Some of them warned for unconscious persuasion through personalised advertising; others were especially prone to situations in which their child's personal information is being misused by dubious individuals, the so-called stranger danger situations (Minkus, Liu, & Ross, 2015). This is in line with previous research that found that parents are more concerned about their children being exposed to situations in which unsuitable sexual, alcoholic, or gambling content is displayed than marketing activities (Newman & Oates, 2014). Parents potentially have a wrong perception about the prevalence of the risk of children being exposed to these stranger danger situations. Warning children for these stranger danger situations is still important, yet, it is far more likely that the online identity of children will be violated by institutions than by dubious individuals. The results of a recent study examining one hundred mobile apps for children showed that 72 apps violated the federal Children's Online Privacy Protection Act law aiming at protecting kids' online privacy (Horner, 2020). The notion of institutional versus social privacy could also be relevant here: Parents rather carry over their concerns regarding malicious activities on the internet to their kids, and children thus seem to be mainly warned for the consequences of reckless information disclosure in situations where the data receiver seems to be criminal, and not for improper data collection and usage by commercial entities. Parental monitoring should therefore go beyond the typical stranger danger situations and should ideally include discussion of proper data management in different types of (commercial) contexts.

6.2. Managerial and Public Policy Implications

All the above considered, an urgent question arising from this article is how children's privacy can be best protected. We suggest an approach that considers at least an interplay of several actors, namely education, clear (and child-friendly) privacy policies, and more strict regulations. Education (in the form of awareness campaigns or educational programmes) about data practices, its related consequences, and the importance of online privacy seems essential, both to children and parents. After all, it is now difficult to recognise (implicit) data collection practices because of its rather invisible processes. Privacy education should ideally be part of broader school-based media literacy programmes. The scope of these programmes should not only include raising awareness about privacy matters, but it should also provide pupils with a better notion of the many different tactics and strategies used by institutions to commercialise users' personal data. In the point of view of media literacy, such knowledge is then an empowering tool enabling users to critically evaluate commercial messages in different types of contexts, both online and offline (Livingstone & Van der Graaf, 2008).

Furthermore, companies should pay more attention to inform internet users, and especially children, about the aims of its (implicit) data practices. This could, in turn, let them make a more informed choice on disclosure. Efforts such as making ostentatious, to-the-point and child-friendly privacy policies and providing alternatives rather than steering them towards disclosing personal data could be done in this matter.

In terms of regulatory implications, this article shows a void in the responsibilities parents legally have over their children's online privacy and their actual skills regarding this topic. While parents expressed privacy concerns (mostly about their children), they do not sufficiently know how to protect their own or their kids' online privacy and find it too burdensome. Therefore, it can be questioned whether today's focus on parents' legal responsibilities (viz. parental consent) should not be shifted to more strict regulations to constrain or even disallow websites to gather children's personal data, or to a focus on providing parents with more clear guidelines and tips on how to protect their own and their children's privacy. Another important suggestion may be that an erasure of data collected from children once every few years should become mandatory for commercial parties.

6.3. Limitations and Suggestions for Future Research

A first limitation lies in the limited number of interviews, and the convenience sample of the study, dominated by female parents and male boys. This gender imbalance may have an impact on the results, as men have been found to adopt technical privacy protection behaviour, such as clearing web browser history and erasing cookies, more than women (Park, 2015). It can consequently be argued that fathers would build in more privacy protective measures for their children than mothers currently do. Moreover, research also suggests that girls perceive more privacy risks and are more concerned about their privacy than boys (Youn & Hall, 2008). To that end, we propose future research to include a more representative sample for both genders. Furthermore, we did not take parents' social economic status and education level into account when recruiting participants for the interviews, although both play a role in parents' self-efficacy on the internet (O'Neill & Dinh, 2012). These factors may thus be important to consider in future research, as they may have influenced the results.

As employing users' personal data for the creation of personalised advertisements is a common business practice, further research can also benefit from more comprehensive insights into the impact of these advertisements among children. In particular, future work could look into how personalisation influences children's brand and ad responses, and how media (or privacy) literacy can empower them when they are confronted with different types of personalised advertisements.

Also, previous research has often suggested to raise privacy awareness among young children, yet, one key finding of this study is that adults are not always fully aware of privacy issues either and lack skills to effectively protect their (children's) online privacy. As today's legislations put parents forward as the primary privacy protective agents for their children (viz. parental consent), some form of privacy education may also be valuable for them. Future work should therefore have a closer look at how this can be best achieved. Formats such as educational training, situational disclosures, and contextual debriefings have all been found very effective in raising *advertising* literacy (De Jans, Hudders, & Cauberghe, 2017; Zarouali, Ponnet, Walrave, & Poels, 2017). It may thus be interesting to explore whether these ways are helpful in raising *privacy* literacy too, and what format works best.

Finally, based on the results of this research, future research should look further than the stranger-danger discourse when examining young children and look into other, and potentially more prevalent, online dangers. Instead, more thorough insights are needed in how children react upon commercial data exploitation and the various consequences for their online data privacy.

Acknowledgments

This research was funded by the Special Research Fund of Ghent University (BOF), grant numbers BOF.STA.2017.0009.01.IV1 (funded doctoral fellowship of the first author) and BOF.2018.0031.01 (funded post-doctoral fellowship of the third author) and the Research Foundation Flanders (FWO), grant number FWO.3E0.2015.0035.01 (funded post-doctoral fellowship of the second author).

Conflict of Interests

The authors declare no conflict of interests.

Supplementary Material

Supplementary material for this article is available online in the format provided by the author (unedited).

References

Anderson, M. (2019). How parents feel about—and manage—their teens' online behavior and screen time. *Pew Research Center*. Retrieved from https://www.pewresearch.org/fact-tank/2019/03/22/how-parents-feel-about-and-manage-their-teens-online-behavior-and-screen-time

Andrews, J. C., Walker, K. L., & Kees, J. (2020). Children and online privacy protection: Empowerment from cognitive defense strategies. *Journal of Public Policy & Marketing*, *39*(2), 205–219.

Babula, E., Mrzygłód, U., & Poszewiecki, A. (2017). Consumers' need of privacy protection: Experimental results. *Economics & Sociology*, *10*(2), 74–86.

Boyd, D., & Marwick, A. E. (2011). Social privacy in networked publics: Teens' attitudes, practices, and strategies. Paper presented at *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, Oxford, University of Oxford, UK.

Brooks, E. I., & Moeller, A. K. (2019). Children's perceptions and concerns of online privacy. In J. Arnedo & L. E. Nacke (Eds.), *Extended abstracts of the Annual Symposium on Computer–Human Interaction in Play Companion Extended Abstracts* (pp. 357–362). New York, NY: Association for Computing Machinery.

Christofides, E., Muise, A., & Desmarais, S. (2012). Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, *3*(1), 48–54.

Clark, L. S. (2011). Parental mediation theory for the digital age. *Communication Theory*, *21*(4), 323–343.

De Jans, S., Hudders, L., & Cauberghe, V. (2017). Advertising literacy training: The immediate versus delayed effects on children's responses to product placement. *European Journal of Marketing*, *51*(11/12), 2156–2174.

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, *33*, 153–162.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16.

Hobbs, R. (1999). The seven great debates in the media literacy movement. *Journal of Communication*, *48*, 16–32.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7

Horner, K. (2020). Researcher develops tool to protect children's online privacy. *Utdallas*. Retrieved from https://www.utdallas.edu/news/science-technology/children-online-privacy-tool-2020

Hudders, L., & Cauberghe, V. (2018). The mediating role of advertising literacy and the moderating influence of parental mediation on how children of different ages react to brand placements. *Journal of Consumer Behaviour*, *17*(2), 197–210.

John, D. (1999). Consumer socialization of children: A retrospective look at twenty-five years of research. *Journal of Consumer Research*, *26*(3), 183–213.

Kirwil, L. (2009). Parental mediation of children's internet use in different European countries. *Journal of Children and Media*, *3*(4), 394–409.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

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. M. Jones & M. Tscheligi (Eds.), *Proceedings of the ACM on Human–Computer Interaction* (pp. 1–21). New York, NY: Association for Computing Machinery.

Lee, S. J. (2013). Parental restrictive mediation of children's internet use: Effective for what and for whom? *New Media & Society*, *15*(4), 466–481.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62–71.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481.

Lievens, E., & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the GDPR. *Computer Law & Security Review*, *34*(2), 269–278.

Livingstone, S. (2004). What is media literacy? *Intermedia*, *32*(3), 18–20.

Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's internet use. *Journal of Broadcasting & Electronic Media*, *52*(4), 581–599.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online? *European Journal of Communication*, *29*(3), 271–288.

Masterman, L. (2003). *Teaching the media*. Abingdon: Routledge.

Mihailidis, P., & Thevenin, B. (2013). Media literacy as a core competency for engaged citizenship in participatory democracy. *American Behavioral Scientist*, *57*(11), 1611–1622.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded source book* (2nd ed.). Thousand Oaks, CA: Sage.

Minkus, T., Liu, K., & Ross, K. W. (2015, May). Children seen but not heard: When parents compromise children's online privacy. In A. Gangemi, S. Leonardi, & A. Panconesi (Eds.), *Proceedings of the 24th International Conference on World Wide Web* (pp. 776–786). New York, NY: Association for Computing Machinery.

Newman, N., & Oates, C. J. (2014). Parental mediation of food marketing communications aimed at children. *International Journal of Advertising*, *33*(3), 579–598.

Ofcom. (2017). Children and parents: Media use and attitudes report. *Ofcom*. Retrieved from https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-parents-2017

O'Neill, B., & Dinh, T. (2012). Digital literacy, digital opportunities (Digital Childhoods Working Paper No. 2). Dublin: Centre for Social and Educational Research.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236.

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258.

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027.

Perner, J., & Lang, B. (1999). Development of theory of mind and executive control. *Trends in Cognitive Sciences*, *3*(9), 337–344.

Pratt, M. G. (2008). Fitting oval pegs into round holes: Tensions in evaluating and publishing qualitative research in top-tier North American journals. *Organizational Research Methods*, *11*(3), 481–509.

Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human–Computer Studies*, *110*, 21–32.

Rozendaal, E., Buijzen, M., & Valkenburg, P. (2010). Comparing children's and adults' cognitive advertising competences in the Netherlands. *Journal of Children and Media*, *4*(1), 77–89.

Shin, W. (2015). Parental socialization of children's Internet use: A qualitative approach. *New Media & Society*, *17*(5), 649–665.

Shin, W., Huh, J., & Faber, R. (2012). Tweens' online privacy risks and the role of parental mediation. *Journal of Broadcasting & Electronic Media*, *56*(4), 632–649.

Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior*, *54*, 114–123.

Smit, E. G., van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, *9*(3), 203–223.

Third, A., Spry, D., & Locke, K. (2013). Enhancing parents' knowledge and practice of online safety: A research report on an intergenerational 'living lab' experiment. Melbourne: Young and Well Cooperative Research Centre.

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 *Reforming European Data Protection Law*, *2015*, 333–365.

Turow, J., & Nir, L. (2000). The Internet and the family: The view from parents, the view from kids. Pennsylvania, PA: Annenberg Public Policy Center—University of Pennsylvania.

Walrave, M., & Heirman, W. (2013). Adolescents, online marketing and privacy: Predicting adolescents' willingness to disclose personal information for marketing purposes. *Children & Society*, *27*(6), 434–447.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12). https://doi.org/10.17705/1jais.00281

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418.

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology & Behavior*, *11*(6), 763–765.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500.

Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior*, *69*, 157–165.

Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M., & Shadbolt, N. (2019). 'I make up a silly name': Understanding children's perception of privacy risks online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). New York, NY: Association for Computing Machinery.

About the Authors

Laurien Desimpelaere is a Doctoral Student at the department of Communication Sciences at Ghent University. Her research interest is situated in the domain of personalized advertising, online privacy, online disclosure behavior in a commercial context, and privacy literacy. Hereby she specifically focuses on children between nine and twelve years old.

Liselot Hudders is an Associate Professor at the department of Communication Sciences at Ghent University and a Postdoctoral Fellow of the FWO at the Marketing department. She conducts research on digital and responsible advertising with a focus on a minor audience.

Dieneke Van de Sompel is a Postdoctoral Researcher at the department of marketing, innovation and organisation and the department of Communication Sciences at Ghent University. Her research interests include the effects of (social) marketing and persuasive communication on children's (consumer) behavior.

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 conceptualizations 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 password 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 figured 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 privacy 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.

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 185–196
DOI: 10.17645/mac.v8i4.3277

Article

Navigating Onlife Privacy: A Family Environment Perspective on Children's Moral Principles

Joke Bauwens [1,]*, Katleen Gabriels [2] and Lien Mostmans [3]

[1] CEMESO, Vrije Universiteit Brussel, 1050 Brussels, Belgium; E-Mail: joke.bauwens@vub.be
[2] Department of Philosophy, Maastricht University, 6200 MD Maastricht, The Netherlands;
E-Mail: k.gabriels@maastrichtuniversity.nl
[3] Office of Research and Innovation, Erasmus Brussels University of Applied Sciences and Arts, 1070 Brussels, Belgium;
E-Mail: lien.mostmans@ehb.be

* Corresponding author

Submitted: 22 May 2020 | Accepted: 4 September 2020 | Published: 10 November 2020

Abstract
This article illuminates which moral principles children and their parents invoke to explain onlife privacy-related practices from a family ecological and narrative approach. It draws on a focused ethnographic study with 10 Flemish socially privileged families with a keen interest in digital technologies and at least one child entering their teenage years. We analyse our data through the analytical lens of a sociopsychological framework that considers children's privacy experiences from three dimensions: self-ego, environmental, and interpersonal. Overall, this article concludes that while risk-averse concerns are present in both the parents' and children's narratives about onlife privacy, parents have allowed their maturing children considerable privacy and leeway. Also, both parents and children articulated the importance of respecting one another's privacy. We frame this set of principles as 'quadruple R': responsibility, risk, reputation, and respect for privacy.

Keywords
children; emerging teenagers; family environment; morality; onlife; privacy

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

Drawing on the plethora of data on teenagers' online privacy practices, on the one hand, and digital parenting, on the other, one cannot but conclude that privacy evokes a wide range of moral considerations (Blum-Ross & Livingstone, 2017; Flores & James, 2013). Our inquiry starts from this observation and argues, in line with others (Jorge & Farrugia, 2017), that in order to understand actual privacy behaviours, the "underlying moral logics in young people's accounts of their practices" (Berriman & Thomson, 2014, p. 583) warrant more in-depth research. Given that family plays a major role in how children and young people learn to deal with media and life (Clark, 2013; Paus-Hasebrink, Kulterer, & Sinner, 2019), this article proposes a context-sensitive ecological perspective, exploring the interaction between families' privacy practices, which are inherently moral, and children's "as both developing beings and active moral agents" (Montreuil, Noronha, Floriani, & Carnevale, 2018, p. 25). We will speak about 'onlife' privacy, emphasising that "the physical and the digital are not separate realms, but jointly part and parcel of the human condition" (Koops, 2018, p. 654).

In doing so, we build on qualitative data that were collected for the PhD study of one of this article's authors (Mostmans, 2017). The research included 10 Flemish socially privileged families with a keen interest in digital technologies. In these families at least one child had just made the transfer from junior to senior school and was about to hit puberty or had just entered his teens; so-called "emerging teenagers" (Paus-Hasebrink et al., 2019, p. 53). From other studies, we know that these families offer an interesting scene for inquiring privacy and the surrounding moral negotiation. With children striving for more autonomy and intense digital media use, these families are increasingly confronted with various turning points, lively debate, unease and concern, also regarding privacy (Kaare, Brandtzaeg, Heim, & Endestad, 2007).

This article aims to contextualise the set of principles children and parents in these families use to navigate onlife privacy. We draw upon a somewhat forgotten, but remarkably topical interdisciplinary framework developed in the 1970s by Wolfe along with her colleagues Laufer and Proshansky, for analysing the different dimensions of privacy in the family context. We bring these dimensions into dialogue with recent studies on how both parents and children enact morality regarding privacy and the Internet.

The first part of the article starts with defining morality, addressing the family as the primary, secure setting for moral socialisation and discussing how emergent teenagers affect the private–public dynamics within families. We then shed light on the three dimensions of privacy, as proposed in the aforementioned analytical framework, and the four key principles that have become apparent in recent studies on young people's narratives of Internet experiences. In the second part, the methodology is explained. The third part unfolds the findings of the study organised along the three dimensions and key moral principles children and their parents fall back on to justify their practices. Overall, we underline the importance of the quadruple R framework within this particular social milieu as a set of moral principles to orient one's own behaviour and interpret that of others.

2. Theoretical Background

2.1. Morality in Family Context

Morality can be defined as a person's negotiation with the values and beliefs that are displayed within a shared culture, community, or group. On an individual level, morality is about evaluating one's own and other's behaviour, principles, judgment, norms, and values. On a social level, morality ties us all to each other and makes it possible to fulfil our strong need to be part of a group. Moral experience, development, and agency are shaped by interpersonal interactions and group involvement (Haidt, 2003; Hitlin & Vaisey, 2010).

Everyday family life is the primary realm of moral experience. It is where morality is recurrently practised, values are learned and tested, and beliefs are given and challenged. Academic literature shows that parents serve as models of morality—in terms of setting the example—for their children (Steinberg & Silk, 2002). Everyday family life "is imbued with implicit and explicit messages about right and wrong, better and worse, rules, norms, obligations, duties, etiquette, moral reasoning, virtue, character, and other dimensions of how to lead a moral life" (Ochs & Kremer-Sadlik, 2007, p. 5). Discursive approaches to morality have demonstrated that moral norms are constantly negotiated and enacted in family interactions (Sterponi, 2003). In narrative psychology, everyday interactions among parents and children are viewed as a key component in the formation of the moral self, for both parties (Pasupathi & Wainryb, 2010). Therefore, what we call morality includes how both children and parents explain, give meaning to, and construct narratives about privacy.

In particular with emergent teenagers who seek to gain autonomy in developing a personal identity, it is fairly common that families have to deal with conflicting perceptions of the moral values surrounding privacy. As children enter adolescence, they gain more independence and aloneness, explore tactics to avoid parental control, negotiate rules with their parents, and see their opportunities for unsupervised interaction with others proliferating, both online and offline, such as on their way to school (boyd, 2014; Zimmer-Gembeck & Collins, 2003). They seek more privacy, for instance in their rooms or by hiding information from their parents, as they hold on to the increasing importance of secrecy (Kaare et al., 2007; Livingstone & Sefton-Green, 2016). A wide spectrum of media practices, such as listening to music, having one's own smartphone, gaming, interacting on social media, accompany this process (Ortner & Holly, 2019). Teenagers use online media, and in particular social media, "to show to peers that they grew out of childhood" (Balleys & Coll, 2017, p. 887). That makes it more difficult for parents to keep up with their children's engagement with the media and, essentially, with others. Especially teenagers' commitment to peer culture, enacted through intensive online interaction, can accelerate processes of distancing in the family (Kaare et al., 2007). Recent studies, however, show that parents are still seen as the source of inspiration and values and families as the beacon of moral guidance (Girsh, 2014; Jorge & Farrugia, 2017).

2.2. A Three-Dimensional Definition of Privacy

Contemporary scholarly work on both digital childhood and children's morality converges on the position that children are participants in their own right who are capable of understanding and experiencing life, but that this cannot be divorced from the sociocultural contexts in which they grow up (Frankel, 2012). The establishment of a child-oriented and ecological approach to privacy can be traced back to Wolfe along with her colleagues (Laufer & Wolfe, 1977; Wolfe, 1978). In their pioneering work, the North American scholars start from a child-centred perspective that stresses the equal importance of "age and age-related experiences" (typically a psychological concern) and the role played by "cultural and sociophysical environmental factors" (a traditionally sociological concern; Wolfe, 1978, p. 175). In more recent scholarly work on childhood, media, socialisation, and development, exactly this dynamic interplay of individual and structural components has become key in understanding children's dealings with digitally networked devices (Paus-Hasebrink et al., 2019). The framework thus provides a good starting point to analyse how emerging teenagers' concepts of privacy are tied to concrete situations in everyday life.

The framework points to three interacting dimensions that shape how young people conceptualise and experience privacy and privacy infringement. It accentuates that these three dimensions are dynamic throughout time and history. Hence, the way people (not only children) alter as they progress through the life cycle influences how they perceive and define privacy. However, larger sociohistorical transformations also outline the paradigms for people's thoughts on childhood, adulthood, parenting, and privacy. Furthermore, the framework acknowledges that the three dimensions are differential across various cultural and social contexts.

First, there is the self-ego dimension of privacy. It shows that the psychological aspects of privacy, such as protecting, nurturing, and enhancing the self, and the possibility of separateness, being and functioning alone, are intrinsically connected with moral values such as personal dignity, freedom to choose your own movement, personal agency for control, and choice over with whom one's personal information is shared (Burkell, 2016). Although not widely accepted, the relationship between respect for children's individuality, privacy, and well-being is a cornerstone in the 2007 World Health Organisation's framework of good parenting and a child's right (cf. United Nations General Assembly, 1989, Art. 16). In Flanders, where this study's data were gathered, The Office of Children's Rights Commissioner, founded in 1997, is active in ensuring this.

This brings us to the second, so-called environmental dimension that shapes which privacy options young people have at their disposal. Here, cultural meanings about privacy, such as mores of a community, cultural meanings, tradition, values, lifestyle, and history play an important role (Laufer & Wolfe, 1977, p. 24). The authors point out that especially culture, which includes cultural imageries about good parenting, family life, or childhood, is a decisive and robust environmental element. Likewise, the interaction between social and physical aspects of environments deserves attention. For example, social arrangements, family composition, types of tasks required (such as studying, working) and rituals (such as family meal, bedtime) circumscribe the available options on which young people are dependent and from which they can draw to give meaning to privacy. These are entangled with physical characteristics of places (such as design, available technologies, and the physical presence of people). Clearly, since then, the public–private boundaries of the family home have changed drastically, not the least with online media. It has become more difficult to prevent the outside world from entering the home, and vice versa—the privacy of the home is easily shared with distant others. Hence, the home and family, typically seen as one of the key private spaces, faces the complexities of interactions stretching out over online and offline contexts (Koops, 2018).

This leads us to the third so-called interpersonal dimension of privacy. This dimension has attracted a dominant focus in scholarly work on young people and online privacy (see for example Zarouali, Poels, Walrave, & Ponnet, 2019). It deals with questions such as what information children choose to share with others about themselves and how they try to learn to be in control of that (e.g., disclosure of personal information). This requires management on a daily basis and produces conflicts with others and with oneself, especially for young people who often face situations that are controlled by adults and technologies. However, child-oriented research indicates that self-disclosure behaviour of young people, often deplored by adults, is a key component in strengthening social ties among peers. By eliciting and providing feedback, support and empathy from and to others, young people construct and explore morality, in terms of belonging, community, the relationship between the self and the other, etc. (Balleys & Coll, 2017; Mostmans, 2017). On the other hand, as their social life is expanding and their moral agency is developing, young people also struggle with finding a balance between the boundaries of online peer groups and personal boundaries (Adorjan & Ricciardelli, 2019).

2.3. Privacy and Morality: The Quadruple R Principles

Notwithstanding the popular image of teenagers' rashness in online privacy matters, studies from the recent past increasingly show that young people care deeply what they want to share about themselves with others (Balleys & Coll, 2017). This sensitivity seems to resonate with the amount and tone of media coverage on online privacy (De Wolf & Joye, 2019) and increasing attention to digital media literacy in education (Pangrazio & Cardozo Gaibisso, 2020). From research on digital parenting, we learn that parents too are sensitive to their children's privacy, not only in terms of protecting their children from malicious intrusion (e.g., predators, harassment) and commercial exploitation (e.g., advertising, tracking, dataveillance), but also in their relationship with their children (Blum-Ross & Livingstone, 2017). Together, these studies seem to suggest that both children and parents mobilise four key categories to orient their conduct and the interpretation of others' conduct, namely: risk, responsibility, reputation, and respect; coined as the quadruple R principles.

First, among children, risk awareness is an important moral compass to fend off dubious digital activities (Adorjan & Ricciardelli, 2019; Berriman & Thomson, 2014). Parents also continue to frame their concerns about their children's online interactions within the wider cultural imaginaries of stranger danger, in which media coverage plays a magnifying role (Drotner, 2013; Leick, 2019).

Second, young people are increasingly encouraged to rely on their sense of responsibility. Stimulating self-reliance is quite common in socially diverse, busy families with teenagers, where moral rules are not always clearly defined and sanctions are rather limited (Frankel, 2012; Livingstone & Sefton-Green, 2016). In turn, emergent teenagers blame peers who experience negative side effects of revealing too much personal information of not being savvy enough or of being vain attention-seekers (Jorge & Farrugia, 2017).

Third, conscious of the potential consequences that their digital performances can have on their reputation, young people demonstrate prudence, both online and offline (Adorjan & Ricciardelli, 2019). Girls are especially sensitive to how their online performances might be received and run the gauntlet of decency by navigating the social and moral complexities of whether or not to share sexually suggestive images of themselves (Ringrose & Harvey, 2015). Parents as well are concerned about the reputational damage of children's online representation (Autenrieth, 2018).

Fourth, maturing children increasingly attach great importance to how other people respect their privacy and take offence at adults (parents specifically) snooping in their personal space and sharing uneasy details about children's personal life online (Lupton & Williamson, 2017). In one of our studies, we found that from the age of nine, children morally disapprove of parents disclosing information about their children without consent (Mostmans, Bauwens, & Pierson, 2014).

3. The Study: Sample, Data Collection, and Analysis

In the study at hand, a focused ethnographic research approach was used (Knoblauch, 2005). Unlike conventional ethnographic work, it focuses on a particular aspect of people's daily life and is characterised by short-term field visits, intensive use of audio-visual technologies of data collection and more delineated time spent in the field (in part-time rather than a permanent researcher presence). The fieldwork was carried out throughout 2013–2015 in Flanders, the Dutch-speaking part of Belgium. The sample consisted of 10 families with at least one child aged 10–14 years living in urban and suburban areas. Although the families varied in terms of family type and composition, all parents shared a keen interest in digital technologies (see Table 1). Some of the parents were tech workers or worked in communications, with advanced media proficiency (Michael Daniels, Julia Philips, Peter and Jill Meyer, Fred Stevens, Daniel Stokman). Others, such as the Bissettes and the Salomons, could be described as 'geeky' families "where digital activities and play are a source of shared enjoyment and learning" (Livingstone & Blum-Ross, 2019, p. 70). The rest of the families balanced between technology-enthused and averse but were nonetheless convinced of the importance of digital media for education, work, society, economy, etc. (the Arnolds family, the Jacobs family, the Mansour family). Overall, the 10 families scored high in terms of educational level or income, and in certain cases, in both areas (see Table 1).

We used different methods of data gathering to contextualise the family's narratives about digital media and privacy. First, through participant observations, we were able to: find out how and where the children used media devices; observe explicit and implicit family (spousal, sibling, parent-child) interactions; make reflective notes on how parents and children communicated with each other about or through media; observe the Internet activities of the children; and audio-record relevant spontaneous talk. For example, we asked them about their recent online activities and experiences (e.g., What did you post online this week, and why? Did you see or experience anything special?), and to take us on a 'digital tour' around their personal and preferred pages. The children led the tours, explaining what they had posted, what they found interesting and fun, and what they did not like so much.

Second, the participant observations formed the starting point of individual ethnographic interviews (with parents and children separately) and group ethnographic interviews (with the family) in the homes of the families. Given our interest in families' narratives, the focus shifted from "what actually happened" to "how people make sense of what happened" (Bryman, 2012, p. 582). During one of the visits, parents and other caretakers were invited to recall how they had experienced privacy as a child. Parents constructed their life story as a reflexive narrative which allowed us to grasp the moral values they believed to be critical and how they came into play in their relationship with their children. While the individual interviews enlightened us about the individual experiences of the children and parents, the group interviews illuminated how a family collectively made sense of onlife privacy. We explained that the interviews could take place anywhere in the house where they felt most comfortable. The majority of interviews took place in the living room or, with some families, in the children's bedrooms. Lastly, to encourage the children's involvement, we used various participatory methods, such as categorising vignettes that described online privacy-related rules and situations; mapping the family's home environment in terms of media devices and public–private boundaries (see Figure 1).

Specifically, the analysis of all data for each family was clustered along two axes. One axis used the three privacy dimensions which functioned as analytical constructs for identifying when, how, and where privacy-related experiences mobilised moral reflection

Table 1. Overview of families.

	🏠	👪	Social milieu
Family 1: Arnolds	Nuclear family	Steve (father), Jane (mother), Tom (male, 12), Alex (male, 10)	Steve, administrator Jane, administrator Double income High income
Family 2: Bissette	Nuclear family	David (father), Vicky (mother), Sophie (female, 13), Anthony (male, 10)	David, museum worker Vicky, administrator Double income High income
Family 3: Daniels	Nuclear family	Michael (father), Jessica (mother), Kenny (male, age 13), Sam (male, 11)	Michael, university degree, IT engineer Jessica, university degree, IT engineer (in-between jobs) Median income
Family 4: Jacobs	Divorced family, 1 single-parent household (Gemma was raising Charlotte; father occasionally came for visits)	Gemma (mother), Charlotte (female, 14)	Gemma, teacher in primary school Stable median income
Family 5: Mansour	Divorced family, 2 single-parent households (Max’ father, William, was not part of the research)	Mina (mother), Max (male, 14)	Mina, university degree, freelance translator, writer and part-time teacher (looking for work) Irregular income
Family 6: Meyer	Nuclear family	Peter (father), Jill (mother), Eliza (female, 13), Ben (male, 11), Charlie (female, 9)	Peter, IT engineer Jill, IT engineer Highly educated Double income High income
Family 7: Montgomery	Stepfamily, 3 households	Denny (male, 14) lives in the Miller and Phillips households (co-parenting arrangement).	
		Vincent (male, 14) lives in the Simmons and Phillips households (co-parenting arrangement).	
		The Phillips household: Walter (Denny’s father), Julia (Vincent’s mother), Kevin (Vincent’s brother, 17, not part of the research)	Walter, executive in IT company Julia, digital marketing manager Double income High income
		The Simmons household: Robert (Vincent’s father, not part of the research), Jennifer (Vincent’s stepmother), Anna (female, 9)	Robert and Jennifer, occupations not available Double income High income
		The Miller household: Nancy (Denny’s mother), Simon (Denny’s brother, 20, not part of the research)	Nancy, teacher in primary school Stable median income

Table 1. (Cont.) Overview of families.

	🏠	👪	Social milieu
Family 8: Salomon	Nuclear family	Oscar (father), Julie (mother), Lucy (female, 16), Harry (male, 13), Luke (male, 10), Trixy (female, 5, not part of the research)	Oscar, attorney and historian, tech worker/creative worker in a digital design agency Julie, attorney; in between jobs at the time of the study Double income High income
Family 9: Stevens	Nuclear family	Fred (father), Gina (mother), Nathan (male, 13), Alexander (male, 9), Ellie (female, 5, not part of the research)	Fred, director sales and marketing in HR software company, digital expert Gina, teacher in secondary school Double income High income
Family 10: Stokman	Stepfamily, 2 households	Daniel (father), Lisa (mother, not part of the research), Rani (stepmother), Daria (female, 10), Thomas (male, 9), Lily (female, 5, not part of the research)	Daniel, tech worker Rani, communication officer in IT research institute Double income High income

Note: All names used are pseudonyms. Both parents and children gave fully informed consent.

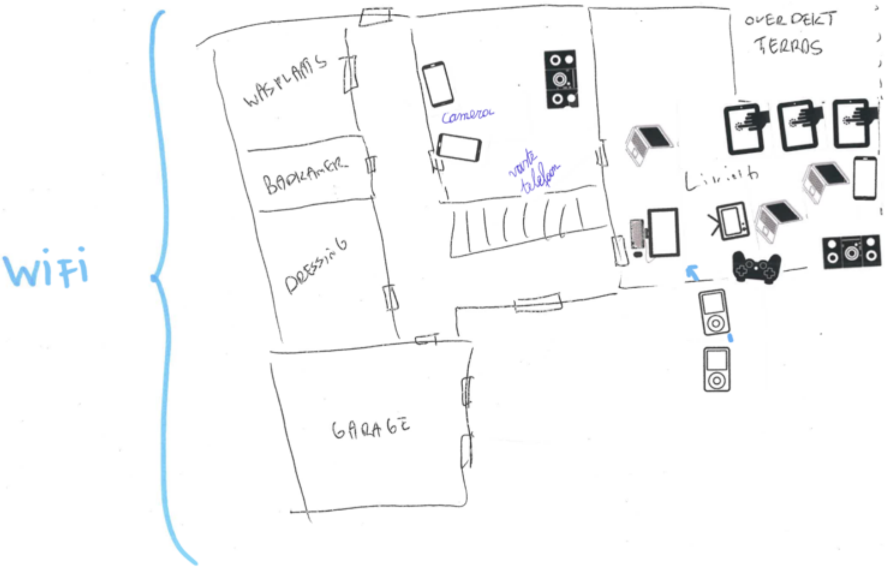

Figure 1. Example of a child's media use map.

and decision-making. The other axis used the quadruple R principles, as explained above, to analyse how and when parents and children invoked them. For example, the following excerpt would be coded as interpersonal and reputation:

> We will regularly have a conversation about that, among others about time. I have talked with him, I said, realise that if you *write* something somewhere that….You know, if you *say* something to someone, that is gone, but if you *write* something it remains visible. On the other side, it may also be read by parents. There were some lame comments, icons like turds and all those things, so it was not at all, how should I say it…shocking or so. But you know, you want to give a guideline….For example, on his mobile phone, he let

> me hear a sound recording of one of his friends farting, if I may say so. Yes, I understand that they are teenagers. But I wouldn't want him to do that to someone else, so these are things I try to talk to him about. (Gina, emphasis added)

In using data analysis software, we were able to obtain an integrated perspective on every single family as well as a comparative perspective on all families involved.

4. Findings

4.1. Respect for Privacy as a Family Rule

Overall, our findings show that privacy is an important value that manifests itself culturally and sociophysically. All parents acknowledged that privacy is a self-evident right, both for adults and children. Apart from Rani, stepmother in the Stokman family, all parents were born and grew up in Flemish families between the late 1960s and late 1980s. However, having been raised in families with different class backgrounds, parents sometimes had dissenting opinions about the boundaries of their own and their children's privacy and had to bring their divergent privacy experiences as children and teenagers in line with one another. Some of the parents recounted a strong sense of privacy in their families (e.g., not opening the mail of others; private bedrooms). Others grew up in families where they had little privacy. For some, this was accompanied by control and distrust by their parents. For example, Rani deplored the fact that she, as an adopted child with two strict parents of older age, was raised in an "overprotective" and "old-fashioned" household and had not enjoyed as much privacy as her peers in her youth. Oscar, the father in the Salomon family, mostly remembered his family's difficult relationship with secrecies; his father being a "closed book" and his "suspicious" mother "always wanting a thousand details." Others who had also experienced little privacy at home did not necessarily have unpleasant memories of their private experiences as a child. They reminisced about their family as a buffer of safety and trust, in which family members were open and transparent (e.g., no locks on the door).

Despite the variety of life stories, all parents presented privacy as a cornerstone of their child-rearing principles. For example, Rani was determined to do things differently with her stepchildren and stressed the idea that good parents "of our time" should respect their children's privacy and allow them some agency in choosing separation from their parents. In this sense, she actively sought to stimulate the children's self-reliance. Returning to the definition of privacy as outlined before, this and similar stories demonstrated how the cultural meanings surrounding privacy, in terms of values and norms, were widely shared within this social milieu.

In combination with most of the families' advantageous living conditions, the opportunities for both parents and children to retreat were plentiful. Apart from Max, all children grew up in spacious, single-family dwellings that offered many opportunities for privacy experiences. Most of the children had their own bedroom (at mother's and father's place if parents were separated), sometimes even their own floor or back house. Some children still shared their bedroom with a sibling but had the prospect of having their own bedroom when they would leave primary school. A wide array of shared devices (such as desktop computers, laptops, television), as well as individually used items (such as smartphones, game consoles, tablet computers, music players), was scattered across pretty much the whole house.

In the various types of family settings we investigated, we found that both parents and children used the potential of their living environment to produce privacy opportunities for themselves. Hence, not only did children report that they retreated into their bedroom or used earphones to create "unbothered" aloneness, parents also described how much they "needed to be on their own." The wish for separateness, typically ascribed to teenagers and problematised as a risk to the family's togetherness (Livingstone & Sefton-Green, 2016), was thus also palpably articulated and practised by the parents. For instance, Mina, a single mother living with her son in a two-bedroom apartment, emphasised the importance of physical withdrawal at home. Other parents claimed the use of technological devices which allowed for psychological rather than physical withdrawal. Earphones proved to be important technologies to enable this kind of separateness. Parents also used these technologies to create "interactional boundaries" (Laufer & Wolfe, 1977, p. 33) in rooms shared with their children.

Given that the children hardly ever recounted conflicts with their parents about privacy, it can be assumed that they felt indeed respected in their right to a certain amount of control and choice in their movements, interaction with others, and information needs. Overall, the children rarely expressed feelings of being in situations that heavily restricted the available forms of privacy in their family environment. Apart from disputes among siblings, sometimes even during the interviews, all children were relatively comfortable about how their family (or families, in the case of separated parents) engaged with their privacy.

4.2. Exceptions to the Rule

Especially with children entering their teenage years, parents expressed their desire for trust and rapport, encouraging their children to share their concerns and disturbing experiences, and at the same time allowing their maturing children privacy. Emotional involvement and trusteeship, often found in research on middle-class families and digital parenting (Livingstone & Blum-Ross, 2019; Naab, 2018; Ortner & Holly, 2019), were accompanied with a firm belief in children's empowerment and self-reliance. In particular parents—fathers mainly and some mothers who were apt consumers of digital media—articulated a deep sense of trust in their children's growing capabilities because of their own personal digital skills to which their children could resort. Overall, mothers displayed less digital self-confidence than fathers but told us that they worked hard to establish a trust relationship with their children. For example, Gina could not imagine how her three children would go about with privacy on the Internet in the near future, but was pretty hopeful that "they will just dare to tell or ask me and then we'll see when the moment is there."

Parents reported that they had invested a lot of effort into teaching their emergent teenager lessons about what to share with whom. For example, they typically used the momentum while creating a social media or game account for their children to talk about privacy and the rules they had to keep in mind. Most of all, parents stressed the importance of working towards open communication and trust. In such a family climate, parents showed a fair amount of trepidation about managing their children's online practices and distanced themselves, mainly mothers, from other mothers who had commented on their so-called "liberal" and "trusting" digital parenting style. For example, Jessica criticised these mothers "for not giving their children enough room to freely explore the Internet," while Gemma accused them of being "not sufficiently emotionally involved with their children, resulting in unpleasant privacy-related experiences."

Although the emergent teenagers were allowed considerable leeway, parental intervention in their privacy was consistently justified based on the same principles. In line with other studies, noted at the outset, concern about risk, responsibility, and reputation functioned as leads for explaining the onlife privacy rules at home. As long as parents intervened in line with these three entangled principles, teenagers would concur with that. For example, Walter instituted the practice of posting a message on his oldest daughter's Facebook timeline when she forgot to close her account after using his laptop. Since there was a heavy sense of taking responsibility for your online privacy in this family, Lucy did not interpret this as an invasion of her privacy by her father but as "her own fault."

But if privacy infringement by the parents could not be accounted for by these principles, emergent teenagers displayed great moral indignation. In the family Daniels, for instance, the oldest son had discovered via his history that his father had snooped into his logged-in Facebook account while working on the shared family computer. His younger brother was immediately on board and shared his brother's anger. So did the mother, who confronted her husband with this privacy intrusion. This incident was told by the mother with a mixture of embarrassment and indignation, as she saw it as a transgression of a clear family norm. She also found it difficult to reconcile the father's behaviour with the family's ideas about parenting which were firmly based on empowering their children by endorsing their self-confidence. Another incident concerned Denny. This boy, with separated parents, was heavily disappointed in his father who had checked private messages on his smartphone without his knowledge and contrasted his father's conduct with his mother's "great respect for his privacy.''

4.3. *'Keep Yourself and the Family Safe'*

Risk of privacy intrusion from outside the family was a main concern in the narratives the families relied on to give meaning to privacy. Interaction with unknown others was regularly mentioned as the first thing they would never do. Adult strangers were especially defined as not trustworthy to share personal information with. Parents pointed at the risk of predators and imprinted their children never to share personal details with unknown others. Daria re-enacted this rule in her own words as "people with bad intentions" and Denny as "people who might seek you out and harass you."

The families were also particularly occupied by the risk of burglary and parents had taught their children never to share online information about home addresses. Nonhuman actors, such as obscure games, shopping, and downloads, were also considered as potential privacy invaders. In this respect, "never disclose contact and banking details to unknown others" was regularly recited as a mantra. These children were raised with the idea that amidst an increasingly insecure and complex world, the family is your stronghold that helps you keep safe, but at the same time needs to be protected as well. Hence, children also were given a share of the responsibility to protect the family against intruders; they articulated a strong sense of co-responsibility in keeping their family safe. This sometimes meant that children did not tell their parents when they experienced privacy invasions on the Internet, fearing that their parents would have called into question their sense of duty, as Thomas explained to us.

4.4. *Care of the Self and Moral Superiority*

Reputation and one's task to watch over this were consistently linked with the self-ego dimension. Personal dignity was a repeated motif in the children's narratives. The emergent teenagers, who were allowed to go on social media when they entered secondary school, were especially conscious about what they would post online and what they would not. As demonstrated in many other studies, constructing 'a sense of self' has become increasingly a matter of digital performances and especially pictures. Parents also demonstrated concern about how they might be portrayed online; sometimes diverging in couples about the acceptability of photos, in terms of whether the other did not come out badly or was not ridiculed. Hence, protecting one's vulnerability and avoiding potential exposure to mockery and rejection were described as the main reasons why they would not share anything about themselves online. For instance, pictures in a swimming suit, asleep in bed, naked in the bath, naked tout court, were all examples of what they "would never share online."

Whereas the children's and parents' narratives on risk were mostly in unison, ideas about reputation could vary greatly. In this respect, the sharenting habits of parents in general and their own parents specifically were criticised. In the family Salomon, for instance, both parents were avid social media users and bloggers who regularly published pictures of their four children without their consent. The three oldest children took no offence in their parents' routine of talking about and sharing these pictures online. However, an old bathtub picture of the oldest daughter with her younger brother Harry as very young children was "unpalatable" from the daughter's viewpoint. The other son Luke was not pleased with a picture that his parents recently posted on Facebook of his brother and him fallen asleep together in the family's guest bed. The children showed sensitivity to embarrassing pictures that might be differently perceived by peers than parents.

Our findings also suggested that "moral judgements are genderised" (Jorge & Farrugia, 2017, p. 286; see also Ringrose & Harvey, 2015). Several examples of gender normativity emerged in our dataset. Fathers were especially concerned about their daughters (Salomon, Stokman). Gender normativity also emerged when sons did not fully conform to prevailing beliefs about masculinity. The 11-year-old son in the family Daniels revealed to "really like" My Little Pony: "I'm like, I want to say it but I just don't dare." The mother was concerned about her son's vulnerability if he shared this online. The son also thought very carefully with whom he would dare to share this online.

Young people manifested a lot of concern about how to protect one's reputation online, and at the same time also disdain for others who, according to them, were too careless with their privacy. When we asked them to give an example, they only involved girls. The older boys in our study, such as Denny, expressed moral disapproval of girls who had published or had been exposed in semi-nude photos, as the following excerpt illustrates:

> In first grade, during the examination period, there was some strange girl in second grade who had posted a nude picture of herself. Well, she didn't post it herself. Apparently, it was her stepsister who had done this….But you do not take nude pictures of yourself, to begin with.

The older girls, such as Charlotte, growing up with her single mother, demonstrated a great sensitivity about which pictures would be morally questionable. In explaining to us what pictures she would never post, she clearly distanced herself from other girls who, according to her, "could do what they like," but that she "would not post beach pictures of herself in a bikini, no thanks," given that "men could see that too."

Similar examples of displaying moral superiority were also found among young children, but more in terms of "stupid children" who do not know that it is not safe to share personal details on the Internet. As found in other studies, the terminology that the children in our study used suggests that young people from dominant backgrounds who are raised in the spirit of empowerment, make themselves morally superior to weaker ones (e.g., Jorge & Farrugia, 2017). Their ideas resonated with how parents talked about other parents, who "have not studied" and therefore "do not know how to assist their children properly" (Rani), and hence "have negative experiences with their children" (Gemma).

5. Conclusions

This study sought to attain a contextualised understanding of family narratives about onlife privacy. More particularly, we wanted to shed light on the nexus between children's and parents' moral accounts. We focused on the family as the prime setting for moral socialisation, including the establishment and negotiation of rules and values surrounding privacy. To this aim, we analysed the data of a focused ethnographic study with 10 families, organised along two axes: (1) the three dimensions of privacy (self-ego; environmental; and interpersonal) and (2) the quadruple R principles (risk, responsibility, reputation, and respect for privacy). The integration was helpful to understand the complexity of family life; it invited us to be attentive to the different dimensions of privacy and myriad moral meanings surrounding it.

There are several limitations to this research. First, although every family and every situation were different, they all were from "dominant backgrounds" (Livingstone & Blum-Ross, 2019), with high financial resources and/or cultural resources and therefore sharing a keen interest in the importance of digital technologies in society. Acknowledging the limitation of only shedding light on this particular social milieu, this study nevertheless contributes to a more in-depth understanding of how dominant narratives on digital media and privacy in western society, circulating in the media, education and policy milieus, are (re)produced in privileged family circles. Against our expectations, given their affinity with digital media, high cultural capital and open-mindedness, the parents in our study mobilised stories on stranger danger, sexual predators, and cyberbullying to explain their practices and attitudes regarding their children's online privacy. Although research has found that liberal parents, as in our study, adopt a more nuanced and critical stance towards moral panics on children (boyd & Hargittai, 2013), we found that even self-confident parents with advanced media proficiency construct their moral narratives within the wider cultural discourses on media and their risks for children. What is more, both parents and their children seemed to rely on these narratives to morally distance from “naïve” and “ignorant” others who failed to handle their onlife privacy properly, despite all the information circulating on the risks of the Internet.

We are also mindful of the fact that, given the ethnographic approach, the study remained necessarily small-scale, impeding us from drawing generalising conclusions for Flemish middle-class families. Finally, the fact that the data go some years back in time, we were not able to touch on more recent developments in technology use, such as online tracking devices, and its potential impact on the rapport between parents and children regarding privacy.

However, in agreement with the underpinning idea of Wolfe’s et al. framework and research on cultural imageries (Leick, 2019), we would argue that culture and the dominant perspectives of the community, to which media narratives are inherent, is a robust environmental element that plays “a decisive role in the way an individual defines privacy situations” (Laufer & Wolfe, 1977, p. 28). Hence, together with recent studies, we found that the children in our study were brought up with solid moral principles that revolve around risk, responsibility, and reputation. First, the shadow of the risk society returned in both the parents’ and children’s narratives. In that connection, the stranger danger mantra came in easily, often based on (news) stories they had heard. Second, parents allowed their maturing children considerable privacy. They gradually maintained more distance and gave increased trust, while stimulating self-reliance. This is compatible with generally accepted ideas about healthy moral development, i.e., to guide children towards autonomy and self-reliance. At the same time, parents also saw it as their children’s task to protect their personal and the family’s privacy, as they had taught them the rules. Third, reputation mainly came to the surface in the children’s experiences. Concerned about the detrimental effects that disclosing pictures or details might have on their image among peers, emergent teenagers were watchful and voiced their discontent vis-à-vis their parents when they had shared an “embarrassing” picture of their children online.

In conclusion, however, we found that respect for privacy is the decisive principle around which both parents and emergent teenagers understand onlife privacy within the family circle. Obviously, privacy-related incidents in family life were reported, but what stuck out is that these incidents were fiercely discussed, indicating that transgressing privacy rules inside the family was something one had to account for. As one of the strongest repeated motifs in the families’ narratives, all parents agreed that good parenting is built on giving trust and autonomy to the maturing child and respecting his or her privacy.

Acknowledgments

The PhD research, on which this article builds, was funded by the Flemish Research Organization (FWO). We would like to thank the families who participated in this study and also to express our gratitude to the reviewers for their useful comments.

Conflict of Interests

The authors declare no conflict of interests.

References

Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite “nothing to hide” online. *Canadian Review of Sociology*, *56*(1). https://doi.org/10.1111/cars.12227

Autenrieth, U. (2018). Family photography in a networked age: Anti-sharenting as a reaction to risk assessment and behaviour adaptation. In G. Mascheroni, C. Ponte, & A. Jorge (Eds.), *Digital parenting: The challenges for families in the digital age* (pp. 219–232). Gothenburg: The International Clearinghouse on Children, Youth and Media & Nordicom.

Balleys, C., & Coll, S. (2017). Being publicly intimate: Teenagers managing online privacy. *Media, Culture & Society*, *39*(6), 885–901.

Berriman, L., & Thomson, R. (2014). Spectacles of intimacy? Mapping the moral landscape of teenage social media. *Journal of Youth Studies*, *18*(5), 583–587.

Blum-Ross, A., & Livingstone, S. (2017). Sharenting: Parent blogging and the boundaries of the digital self. *Popular Communication*, *15*(2), 110–125.

boyd, d. (2014). *It’s complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

boyd, d., & Hargittai, E. (2013). Connected and concerned: Variation in parents’ online safety concerns. *Policy & Internet*, *5*(3), 245–269.

Bryman, A. (2012). *Social research methods*. Oxford: Oxford University Press.

Burkell, J. (2016). Remembering me: Big data, individual identity and the psychological necessity of forgetting. *Ethics and Information Technology*, *18*(1), 17–23.

Clark, S. L. (2013). *The parent app: Understanding families in the digital age.* Oxford: Oxford University Press.

De Wolf, R., & Joye, S. (2019). Control responsibility: The discursive construction of privacy, teens, and Facebook in Flemish newspapers. *International Journal of Communication*, *13*, 5505–5524.

Drotner, K. (2013). The co-construction of media and childhood. In D. Lemish (Ed.), *The Routledge international handbook of children, adolescents and media* (pp. 15–22). Abingdon: Routledge.

Flores, A., & James, C. (2013). Morality and ethics behind the screen: Young people’s perspectives on digital life. *New Media & Society*, *15*(6), 834–852.

Frankel, S. (2012). *Children, morality and society*. Basingstoke: Palgrave MacMillan.

Girsh, Y. (2014). The (late?) modern family: The family’s significance for adolescents in Germany and Israel. *Journal of Adolescence*, *37*, 863–870.

Haidt, J. (2003). The moral emotions. In R. J. Davidson, K. R. Schere, & H. H. Goldsmith (Eds.), *Handbook of affective sciences* (pp. 852–870). Oxford: Oxford University Press.

Hitlin, S., & Vaisey, S. (Eds.). (2010). *Handbook of the sociology of morality*. New York, NY: Springer.

Jorge, A., & Farrugia, L. (2017). Are victims to blame? Youth, gender and moral discourse on online risk. *Catalan Journal of Communication & Cultural Studies*, *9*(2), 285–301.

Kaare, B. H., Brandtzaeg, P. B., Heim, J., & Endestad, T. (2007). In the borderland between family orientation and peer culture: The use of communication technologies among Norwegian tweens. *New Media & Society, 9*(4), 603–624.

Knoblauch, H. (2005). Focused ethnography. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *6*(3), Art. 44. Retrieved from https://www.qualitative-research.net/index.php/fqs/article/view/20/43

Koops, B. K. (2018). Privacy spaces. *West Virginia University Law Review*, *121*(2), 612–665.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *3*(3), 22–42.

Leick, K. (2019). *Parents, media and panic through the years: Kids those days*. Cham: Palgrave Pivot.

Livingstone, S., & Blum-Ross, A. (2019). Parents' role in supporting, brokering or impeding their children's connected learning and media literacy. *Cultural Science Journal*, *11*(1), 68–77.

Livingstone, S., & Sefton-Green, J. (2016). *The class: Living and learning in the digital age*. New York, NY: New York University Press.

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, *19*(5), 780–794.

Montreuil, M., Noronha, C., Floriani, N., & Carnevale, F. (2018). Children's moral agency: An interdisciplinary scoping review. *Journal of Childhood Studies*, *43*(2), 17–30.

Mostmans, L. (2017). *Under the radar: Preadolescents' moral conceptions about online self-disclosure* (Unpublished doctoral thesis). Vrije Universiteit Brussel, Brussels, Belgium.

Mostmans, L., Bauwens, J., & Pierson, J. (2014). "I would never post that": Children, moral sensitivity and online disclosure. *Communications*, *39*(3), 347–367.

Naab, T. (2018). From media trusteeship to parental mediation: The parental development of parental mediation. In G. Mascheroni, C. Ponte, & A. Jorge (Eds.), *Digital parenting: The challenges for families in the digital age* (pp. 93–102). Gothenburg: The International Clearinghouse on Children, Youth and Media & Nordicom.

Ochs, E., & Kremer-Sadlik, T. (2007). Introduction: Morality as family practice. *Discourse & Society*, *18*(1), 5–10.

Ortner, C., & Holly, S. (2019). A question of commitment, attention and trust: The role of smartphone practices for parent-child relationships in adolescence. *Kommunikation.medien: Open-Access-Journal für den wissenschaftlichen Nachwuchs*, *10*. https://doi.org/10.25598/jkm/2019-10.8

Pangrazio, L., & Cardozo Gaibisso, L. (2020). Beyond cybersafety: The need to develop social media literacies in pre-teens. *Digital Education Review*, *37*, 49–63.

Pasupathi, M., & Wainryb, C. (2010). Developing moral agency through narrative. *Human Development*, *53*, 55–80.

Paus-Hasebrink, I., Kulterer, J., & Sinner, P. (2019). *Social inequality, childhood and the media: A longitudinal study of the mediatization of socialisation*. London: Palgrave Macmillan.

Ringrose, J., & Harvey, L. (2015). Boobs, pack-off, six packs and bits: Mediated body parts, gendered reward, and sexual shame in teens' sexting images. *Continuum: Journal of Media & Cultural Studies*, *29*(2), 205–217.

Steinberg, L. D., & Silk, J. S. (2002). Parenting adolescents. In M. Bornstein (Ed.), *Handbook of parenting* (Vol 1, pp. 103–133). Mahwah, NJ: Erlbaum.

Sterponi, L. (2003). Account episodes in family discourse: The making of morality in everyday interaction. *Discourse Studies*, *5*(1), 79–100.

United Nations General Assembly. (1989). Convention on the rights of the child. In *Treaty series* (Vol. 1577, p. 3). New York, NY: UN General Assembly. Retrieved from https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&lang=en

Wolfe, M. (1978). Childhood and privacy. In I. Altman & J. F. Wohlwill (Eds.), *Children and the environment* (pp. 175–222). New York, NY: Plenum Press.

Zarouali, B., Poels, K., Walrave, M., & Ponnet, K. (2019). The impact of regulatory focus on adolescents' evaluation of targeted advertising on social networking sites. *International Journal of Advertising*, *38*(2), 316–335.

Zimmer-Gembeck, M. J., & Collins, W. A. (2003). Autonomy development during adolescence. In G. R. Adams & M. Berzonsky (Eds.), *Blackwell handbook of adolescence* (pp. 175–204). Oxford: Blackwell Publishers.

About the Authors

Joke Bauwens is a Professor of Media and Communication Studies at Vrije Universiteit Brussel, Belgium, where she heads the research centre for Culture, Emancipation, Media and Society. Drawing upon sociological and philosophical approaches, her research interests and expertise includes the social, cultural and moral consequences of media. She has published on children's and young people's engagement with media, the relationship between digital media and morality, and the digitisation of media, culture and social life.

Katleen Gabriels is a Moral Philosopher, specialised in Computer and Machine Ethics. She is an Assistant Professor at Maastricht University (the Netherlands), where she is also the Program Director of the BA Digital Society. She is an Executive Board Member of INSEIT, Steering Committee Member and the Deputy Chair of ETHICOMP and an Affiliate Member of 4TU Centre for Ethics and Technology. She is the Author of *Regels voor robots* (2019, VUBPRESS; the English version, *Conscientious AI: Machine(s) Learning Morals*, is forthcoming in 2020).

Lien Mostmans holds a PhD in Media and Communication Studies, obtained in 2017 at Vrije Universiteit Brussels, Belgium. She has extensive research experience in the field of children and media cultures, using a wide range of qualitative (ethnographic, visual) methodologies. Since 2018, she has been working as Research Advisor for Erasmus Brussels University of Applied Sciences and Arts, Belgium, where she coordinates international research projects in the fields of children, education, and healthcare.

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 197–207
DOI: 10.17645/mac.v8i4.3407

Article

Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy

Mariya Stoilova [1,*], Sonia Livingstone [1] and Rishita Nandagiri [2]

[1] Department of Media and Communications, London School of Economics and Political Science, London, WC2A 2AE, UK; E-Mails: m.stoilova@lse.ac.uk (M.S.), s.livingstone@lse.ac.uk (S.L.)
[2] Department of Methodology, London School of Economics and Political Science, London, WC2A 2AE, UK; E-Mail: r.nandagiri@lse.ac.uk

* Corresponding author

Submitted: 30 June 2020 | Accepted: 14 September 2020 | Published: 10 November 2020

Abstract
How do children understand the privacy implications of the contemporary digital environment? This question is pressing as technologies transform children's lives into data which is recorded, tracked, aggregated, analysed and monetized. This article takes a child-centred, qualitative approach to charting the nature and limits of children's understanding of privacy in digital contexts. We conducted focus group interviews with 169 UK children aged 11–16 to explore their understanding of privacy in three distinct digital contexts—interpersonal, institutional and commercial. We find, first, that children primarily conceptualize privacy in relation to interpersonal contexts, conceiving of personal information as something they have agency and control over as regards deciding when and with whom to share it, even if they do not always exercise such control. This leads them to some misapprehensions about how personal data is collected, inferred and used by organizations, be these public institutions such as their schools or commercial businesses. Children's expectation of agency in interpersonal contexts, and their tendency to trust familiar institutions such as their schools, make for a doubly problematic orientation towards data and privacy online in commercial contexts, leading to a mix of frustration, misapprehension and risk. We argue that, since the complexity of the digital environment challenges teachers' capacity to address children's knowledge gaps, businesses, educators, parents and the state must exercise a shared responsibility to create a legible, transparent and privacy-respecting digital environment in which children can exercise genuine choice and agency.

Keywords
children; digital environment; data; datafication; digital by default; media literacy; peer learning; privacy

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

Children's lives are traditionally conceptualized as part of the private sphere, supposedly protected from the public and commercial spheres by the actions of parents, teachers, and other carefully vetted adults. This is meant to ensure their safety and well-being, allowing them to 'just be children.' But today children are a major source of data in a hugely profitable data marketplace (Zuboff, 2019). Their lives are, arguably, becoming datafied—meaning that their possibilities for action, and the affordances of their lifeworld, are influenced by practices of data processing determined by commercial and political priorities far beyond the control or knowledge of a child (Barassi, 2019; Lupton & Williamson, 2017; Mascheroni, 2018). This raises urgent questions about their privacy (Barassi, 2019; Buitelaar, 2018).

UNICEF (2018) distinguishes several dimensions of privacy affected by digital technologies—physical, communication, informational and decisional privacy.

Physical privacy is violated in situations where the use of tracking, monitoring or live broadcasting technologies can reveal a child's image, activities or location. Threats to communication privacy relate to access to posts, chats and messages by unintended recipients. Violation of information privacy can occur with the collection, storage or processing of children's personal data, especially if this occurs without their understanding or consent. Finally, disruptions of decisional privacy are associated with the restriction of access to useful information or the operation of automated decision-making which limit children's independent decision-making or development.

We are reaching the point, especially in wealthier countries, where children's lives can be called digital-by-default: Even before birth they may have a digital profile generated by their parents, a health record produced by the state, and they may have attracted the interest of commercial actors. Thereafter, much of what they do and what happens to and around them will be digitally recorded, enriching that profile and potentially shaping their life chances. Digital-by-default is increasingly the policy of national governments, resulting in a shift away from (expensive) in-person state provision (for example, for paying taxes, claiming welfare or interacting with authorities) towards online-only services. Until recently, concerns with this policy focused on digital exclusion (Schou & Svejgaard Pors, 2019), but increasingly concerns arise for those who are digitally included—regarding their privacy, and the potential for discriminatory decision-making, as recently resulted from the algorithmic calculation of UK students' A-level results.

The more complex, risky and potentially exploitative the digital environment, and the powerful players that own much of its infrastructure, the greater the public call for stronger data protection regulation, privacy-by-design, data justice and a platform duty of care, as well as for digital literacy education for the public (LSE Truth, Trust and Technology Commission, 2018). Children are widely recognized as being among the most vulnerable, justifying calls for stronger privacy legislation. At the same time, children can benefit from digital literacy education, leading to hopes that they can be taught to be savvy and resilient in a digital world, and even to critically understand the modus operandi of the networked data economy (Buckingham, 2015; Culver & Grizzle, 2017; Livingstone, Stoilova, & Nandagiri, 2020). However, insofar as the digital environment is not designed or regulated to be legible and respectful of children's rights or best interests (Buitelaar, 2018) these hopes may be unrealistic.

Both regulation and education policies rely on assumptions about what children can understand or withstand. Our aim in this article is to examine what children can and do understand about online data and privacy, and how they learn about this, in order to inform the balance between regulatory and educational policies and to protect children's privacy online. Such a holistic approach, involving both regulatory and educational solutions aimed at empowering children and safeguarding their privacy and other rights, is increasingly advocated by a rights approach to privacy (Lievens, Livingstone, McLaughlin, O'Neill, & Verdoodt, 2018; Lupton & Williamson, 2017; UNICEF, 2018).

2. Theorizing Privacy in Relation to the Digital Environment

Westin (1967) explains privacy as the right of individuals, groups or institutions to determine if, when and to what extent information about them is shared with others. In popular discourse also, "privacy is understood almost universally as a matter of controlling one's own data" (Sarikakis & Winter, 2017, p. 1). However, the emphasis on individual control gives rise to many difficulties, not least because social life is relational (Solove, 2015) and subject to context-dependent norms (Nissenbaum, 2010). Mulligan, Koopman, and Doty (2016) argue that privacy is "essentially contested" because it must be persistently and adversarially debated and defended. Certainly, it is being intensely debated and defended in relation to the digital environment (Sarikakis & Winter, 2017), including in relation to children (Kidron, Evans, & Afia, 2018; Livingstone, 2018).

While the origins of the concept of privacy can be traced historically, Laufer and Wolfe (1977) offer a developmental account, tracing its meaning and importance to the early life of the infant, showing how privacy is vital to and inseparable from the individuation of the self during childhood. Consistent with contextual and relational accounts of privacy in legal theory, they offer an account of privacy in which the child's developing efforts to manage information are rooted in their growing capacity to manage social interaction. This capacity is always contextual and "it is not until long after the child has learned that he/she has choice that he/she can control access to himself/herself in a way that makes choice meaningful" (Laufer & Wolfe, 1977, p. 39). Positing a lag between the recognition of choice and the capacity to enact choice is particularly thought-provoking now that children spend so much time in a complex and opaque digital environment that offers them little genuine choice or control, and that substantially disintermediates their parents and other protective adults.

Neither a universalist approach centred on individual control nor a highly contextualist approach to privacy is practical when it comes to protecting children's privacy in the current commercialized digital environment. Hence, we work with a more practical classification that prioritizes three digital contexts, informed by Nissenbaum's (2010) idea of contexts as social spheres. Specifically, we propose that children's lives are primarily framed by three social spheres in which privacy matters: interpersonal (family, peers, community); institutional (such as the school or health service); and commercial (notably purchasing, marketing and data brokering). Building on the work of van der Hof (2016), we also distinguish three types of data in the digital environment: data given (contributed by individuals about themselves or about others, usually knowingly, although not necessarily intentionally, during their participation online); data traces (which are left, mostly unintentionally and sometimes unknowingly, through online activities and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata); and inferred data (derived from analysing data given and data traces, often through the use of algorithms, possibly combined with other data sources, and also referred to as 'profiling').

We suggest that data functions rather differently in each of these three privacy contexts: In interpersonal contexts, data meaningfully given is the prototypical case; in institutional contexts, data is often collected—as children know from their school or medical records—although often not fully analysed (Selwyn, 2019); in commercial contexts, the really valuable data is not that given, nor even that taken, so much as the data that is then inferred, aggregated and used to generate profiles in order to target advertising or for other profitable purposes within the networked data ecology (Lupton & Williamson, 2017; Marwick & boyd, 2014; Stoilova, Nandagiri, & Livingstone, 2019). Given that our stated aim is to examine whether, what and how children understand online data and privacy, Laufer and Wolfe's emphasis on the development primacy for privacy of interpersonal contexts gains a new significance in a digital world in which institutional and commercial actors have far greater access to children's actions as mediated through data processing. Available evidence already suggests that children's knowledge of interpersonal contexts for privacy online exceeds that of other contexts (Barassi, 2019; Kumar et al., 2017; Stoilova et al., 2019). It seems that children largely regard the digital environment as a 'personal space' for self-expression and socializing and that, while children are often concerned about parental intrusion into their privacy, or with the interpersonal risks that arise when personal information circulates among peers without their consent, they have little awareness of future implications of data traces, particularly in relation to a distant future that is hard to predict or to conceive of (Bowler, Acker, Jeng, & Chi, 2017; Murumaa-Mengel, 2015; Pangrazio & Selwyn, 2018). Even by the time they reach adolescence, children have little knowledge of data flows or of infrastructure—they mostly see data as static and fractured, as when located on different platforms (Bowler et al., 2017), which can create a false sense of security.

3. Methodology

We conducted 28 mixed-gender focus groups with children aged 11–16 years from six UK secondary schools, two in London and one each in Essex, the Midlands, Wales and Scotland, selected to represent a mix of achievement and geographical area. The 169 participants (85 girls and 84 boys) were selected by their own schools from among those who volunteered after receiving an information sheet about the project, on the basis of diversity in background, grades and digital skills. The project was approved by LSE's Research Ethics Committee and consent was given by the children and one of their parents. The focus groups lasted 73 minutes on average and were held with three school year groups—aged 11–12 years, 13–14 years and 15–16 years.

We designed and piloted participatory research tools (visuals, games, pen-and-paper tasks, workshop activities) to engage students, using real-life scenarios and exemplar digital experiences. To allow children's understanding to emerge spontaneously, we structured the discussion using a 'ladder approach,' starting with more familiar issues and moving towards greater complexity as regards both the privacy contexts and the types of data we invited children to consider. We first invited children's spontaneous perceptions and practices (e.g., apps selection, checking age restrictions, reading terms and conditions), followed by a game to gauge their familiarity with relevant terminology (e.g., cookies, privacy settings, digital footprint, algorithms). Then we conducted exercises to explore the types of data children share in different contexts, gradually enabling discussion of less thought-of issues relating to data harvesting and profiling. Activities were conducted collectively, some in smaller groups, in order to generate conversation and avoid any perception of being tested. All sessions were recorded, transcribed and analysed using thematic analysis with NVivo.

4. What Do Children Know about Data and Privacy Online?

4.1. Interpersonal Contexts: Using the Familiar as a Model

It was immediately apparent that children find it easier and more obvious to focus on interpersonal aspects of online privacy. This is more familiar and understandable to children and it is also the sphere where they have more agency and control. Children were keen to describe their privacy strategies in terms of the way they handle the data they know they give—the pictures they post online, the links they share, the information they enter when registering for platforms—in order to protect their privacy, relationships and reputation. They told us how they remove unwanted information, untag content, use 'fake' personal data, switch between accounts and platforms and use assorted privacy settings and passwords to protect their devices and data. Children's actions of deciding what to disclose, where and to whom, and of negotiating with others what should be shared online, emphasize how they value individual control, and their nuanced appreciation of context, which results in considerable personalization of their choices and tactics.

In dealing with their interpersonal privacy, children acknowledge that they do not have full control over their data because of what Marwick and boyd (2014) describe as 'networked privacy,' referring to the public-by-default nature of online communications. Thus, children realize that others could share information about them without permission or beyond the intended purpose or audience: Parents sharing embarrassing pictures with relatives or friends is a frequent example of how children feel their privacy is breached. Data traces and inferred data appear to be much less significant for interpersonal privacy contexts, although children sometimes mention these in relation to how their information will be perceived or used by others—their parents might track their location when they are late home from school, a burglar could see that they are not at home when they check in to a holiday destination, some of their distant friends will figure out that they were not invited to a birthday party.

Perpetrators of privacy risks are also thought of in interpersonal terms—the stalker, the hacker, the bully, the kidnapper, the 'paedo' (Livingstone, 2014), and children's thinking often revolves around 'what's the worst that can happen':

> People could find out where you go. So they could try and find you and wait for you there. (Boy, Year 7, Essex)

> The only thing that worries me is weird folk, like stalkers. (Girl, Year 11, Scotland).

Indeed, interpersonal risks seem to them much more salient than institutional risks, or long-term risks associated with the commercial data ecology, as already pointed out by previous studies (Barassi, 2019; Bowler et al., 2017; Kumar et al., 2017; Livingstone, 2019; Lupton & Williamson, 2017; Selwyn, 2019). Fewer studies have as yet explored children's understanding of institutional or commercial privacy, so we devote more attention to these in what follows. As we seek to show, because children learn first about interpersonal privacy, it appears that they extend interpersonal assumptions to institutional and commercial contexts. Specifically, we observed how they tend to apply attitudes to privacy—along with their analysis of privacy risks and privacy strategies—from the interpersonal context to a context which is quite different from their initial point of reference. Importantly, as we also demonstrate in what follows, drawing on interpersonal notions of privacy leaves children at a disadvantage in an institutional or commercial environment.

4.2. Institutional Privacy: Symbolic Boundaries and The Role of Trust

When asked about privacy online, children rarely think about institutional contexts or the data that their school, doctor, government, or future employer might hold. Similarly, when talking about personal data, children rarely refer to their immunization or dental records, or school academic achievement or attendance records. We found children rather bewildered when we first mentioned such data, as this is neither information they choose to share nor something they could refuse to give. Perhaps because they have very little control of what is collected by institutions, or of how or when this is collected, they do not grasp immediately that, beyond the data they have knowingly given, these data records are also personal data with significant privacy implications. After all, such information is collected about everyone and some of it—their dental records, for instance—may not immediately seem very telling about who they are as a person. Yet, over the course of our conversations, children realized that the handling of such data could have significant repercussions (for example, if it is stolen or used outside its intended purpose) and, thereby, that a range of institutions that they had not previously given much thought to gather considerable amounts of sensitive data about them.

In relation to institutional contexts, children find it easiest to understand that of the school, which they know holds a lot of their personal information—provided by students and parents or collected by schools. Even the youngest children we spoke to (11–12 years) could list data such as their names, photographs, attendance records, fingerprints (in schools that use this for lunch payment), health information and, on reflection, what they eat for lunch. Rarely a cause for concern, this institutionalized data collection is viewed as justified for ensuring children's health, safety, learning or wellbeing, provided its use is limited to the original purpose. As one boy (Midlands, aged 11–12) explained, "they're my school, they're going to keep my data safe." This comment reflects the importance of trust: The negotiation of trust is traditionally emphasized by theories of privacy (Petronio, 2002), although it is noteworthy that children learn to trust in the context of interpersonal relations (Davis & James, 2013; Kumar et al., 2017) and only later extend this to certain institutional or commercial contexts.

Institutional data collection typically occurs within a broader regime of monitoring, supervision and surveillance. Because it is, in effect, part of 'ordinary' practice, it rarely provokes privacy considerations. In other words, children's understanding of the school's data processing is embedded in their everyday social relations with teachers and school administrators, as well as in the implicit sanctioning of such relations by their parents and peers. For example, children expect to be monitored both digitally and offline to ensure their compliance with an established code of behaviour. Children talked of how their searches and the websites they visit on school computers are monitored:

> The teachers will tell us, they're watching what you're doing. (Boy, 15–16 years, Essex)

> If I need to put sexual health clinic or something and then it blocks it, which is annoying. (Girl, 15–16 years, Essex)

This ‘privacy licence,’ however, is not without limitations. Children expect institutional monitoring to occur within certain physical and symbolic boundaries—on school premises and in relation to educational activities. Or, in relation to health, in the doctor’s surgery or other relevant places. Beyond these boundaries, children expect to retain their privacy. The same teacher who can check what children search for online on the school computer cannot follow them on social media or monitor their social life in their ‘private time’: “Teachers can’t talk to students outside, on social media and so on” (boy, 15–16 years, Midlands).

In short, children’s trust in their schools gives them confidence that their teachers—and the digital apps they deploy at school (homework apps, learning software, etc.)—store their data securely within the school and would not share it further without their permission. However, when we inquired further, children realized they had little knowledge of how their schools use their data, or whether it is shared with third parties, or stored in ways that could not be hacked or breached. Their willingness to trust the school—albeit without much alternative—and their acceptance that they could hardly challenge the decisions made by the school, sets up a particularly problematic reference framework insofar as children apply this to the even more instrumental relationships that characterize the commercial domain (Steeves & Regan, 2014). We explore this below.

4.3. Commercial Privacy: A One-Dimensional Relationship

Commercial contexts are the least likely to be on children’s radar when they think about privacy (Davis & James, 2013). Children are less familiar with how processes operate in these contexts and less able to conceive of their personal implications. Further, in discussing the activities of businesses, some children appeared more able than others to grasp the complex ways in which their data flows online, as well as more aware of the implications arising from the commercialization of personal data. This was partly a matter of age and maturity (Kumar et al., 2017), and also of digital expertise; we also saw hints that critical discussion at school or in the home make a difference to how well children navigate the more complex features of data and privacy online, particularly in relation to commercial contexts.

We found that most children understand that they are targeted with advertising content. They know companies are trying to gain their attention for commercial purposes and are beginning to grasp the mechanics behind content personalization (Davis & James, 2013). For example, most children see connections between the information they are shown and their previous actions—past searches, pages visited, content engaged with. While some understand the functionality behind personalization of commercial content and how cookies support that, more are puzzled:

> Sometimes I get stuff that I’ve already searched. (Girl, 15–16 years, Scotland)

> I’m not entirely sure what it [cookies] means. But, I think, it’s, like, a good thing if you agree though. (Boy, 11–12 years, Essex)

Some children are critical and disapprove of the online business model, but most see it as a necessary compromise in exchange for ‘free Internet’ or just how things are. Some even suggested that personalized advertising content creates a better online experience, presumably trusting commercial messages. Few children made the ‘jump’ from giving an account of targeted advertising to recognizing the algorithmic reshaping of the online environment. Nor did most consider how the same principles of personalization might have wider implications, biasing their online experience or differentiating it from that of their peers or others. In short, children tend to miss the ‘bigger picture,’ as most are not told or taught how such processes might influence their learning, exposure to diversity, choices or decision-making.

Children also struggle with the idea that their online activities produce data traces that permit further inferences about them. Many understand that their actions leave traces online, but what that data is and where it goes is perplexing and made even more complicated by technological innovation, differences across platforms, and non-transparent policies:

> [Talking of a map app]…it will know what trips I’m taking, without me saying. (Girl, 15–16 years, Essex)

> It’s when you go onto websites and stuff and you leave traces, like what you looked up. Like a footprint, but it’s digital. (Girl, 11–12 years, London)

Even though their search history is not data that they have given voluntarily, it is still related to their actions online, so children have a sense of what these actions are and sometimes use strategies to remove or protect such data and their privacy, for example by using incognito tabs or deleting their history. It is much harder for them to grasp the harvesting of data that is not connected to intentional activities—for example, IP address, device information, browser type, time spent on a page. Most children are surprised to learn that such data is gathered, or that it has value for companies.

Understanding how data flows are merged into a digital footprint is too complex for children, as for most adults. The depth and extensiveness of data profiling within a commercial data ecology is too far removed from their experience. Children have only a rough sense of being monitored online, and our focus group discussions led them to raise many questions about how, why and for what purpose this occurs. For instance, asking whether their own deleting of their data means that it is removed permanently from the Internet sparked many debates as children struggled to grasp the idea of a growing digital footprint that is durable, searchable and virtually undeletable. Yet, some experiences give them hints that their online activities leave a permanent trace, as one girl explained: "If you deactivate your [Instagram] account, you just log in and it reactivates it….All your posts come back, and people you follow" (girl, 15–16 years, Scotland).

Most experiences, however, teach them that they have little power to manage the commercial environment. With their privacy settings, data protection choices or other design options, children find in practice that they have little choice but to consent to default options. Each app and platform functions differently from the next, privacy settings change when software updates are implemented, and protecting one's privacy becomes like a game of tag. Tricked by deceptive design (Kidron et al., 2018), children tend to assume that providing personal information when asked is mandatory. Incomprehensible terms and conditions that need to be accepted in order to use a service and cookies that are hard even for a diligent adult to disable teach children that exchanging data for access is unavoidable.

Although the news media make children increasingly aware of data breaches and fraud—children were keen to share recent instances in the focus groups—for the most part, their lack of meaningful choices or forms of redress undermines children's agency in the digital environment. It is in this context that we observe their willingness to trust companies. In practice, they have little option if they wish to use an online service, but in their talk they appeared to draw on their familiarity with interpersonal relationships in explaining why they trusted a company with their personal information:

> If you have friends who have it, then…you trust the app. (Girl, 15–16 years, Scotland)

> If it's like a trusted website that I like, I visit often and trust and all. If it's a big corporation like Adidas or Apple for instance. (Boy, 13–14 years, London)

In other examples, children talked of 'the people' at Instagram, or a friend's father in the tech industry, assuming that the company would act with the same values as would someone they know personally. Or, because they themselves feel offended that 'others' collect their 'private' data, they assumed that those others, be they individuals or companies, would feel it improper to keep or share their data. Or, again, they talked as if the privacy tactics, workarounds and deceptions that they use to protect their online privacy from their friends or parents (such as giving a false name or age, searching 'incognito,' or switching devices) would also protect them from online businesses (or, indeed, institutions).

5. Children's Capacity to Learn about Data and Privacy Online

How can children gain a deeper and more critical understanding of their privacy online not only in interpersonal contexts but also in institutional and commercial ones? In a rapidly changing technological environment, digital literacy—broadly, the knowledge that children need in order to act effectively in relation to the digital environment—is a moving target. Children must summon all their resources to keep on top of new developments, devices, functionality, policies and regulations. Formal education is an important source of information for them, but it is only one form of learning—in many cases children are working it out on their own. However, in trying to put the pieces of the puzzle together from diverse sources of information, children acquire fragmented knowledge, including some misconceptions. Insofar as both children's capacities and the practice of digital literacy education face real limitations, regulatory and/or design solutions for the protection of children's privacy in relation to the digital environment will be necessary.

5.1. Learning by Doing: Working It Out

In their engagement with technologies, children take a hands-on approach—trying things out, learning by doing, and quickly moving from one app to another in pursuit of something new and exciting, while speculating amongst themselves as to where the risks are and what the possibilities may be (Livingstone, 2014). Their digital lives are dynamic and so is their approach to learning about privacy. Children sense—or are working out—that everything they do online may be tracked and recorded for whatever purpose by businesses, parents and schools. While children might ask a parent, a sibling, or a knowledgeable friend to help them, many expect to learn on their own by trial and error or by searching online for information when needed. Children are quite confident about their own abilities to navigate Internet-related issues, while asking adults for help is reserved for 'really serious' situations. Children enjoy exploring new opportunities, following up on things they have heard about from friends, checking out new gossip or trends, or following their favourite popular online figures. These practices are fun and informative and a great way to learn actively. They are also a coping mechanism in a rapidly-changing, hard-to-predict environment with few knowledgeable authority figures in children's immediate surroundings:

> I think ourselves are our best teachers because we learn, and we kind of know. (Boy, 15–16 years, Essex)

> It’s so new that no one really knows what’s going to happen it. No one knows where it’s going to go. (Girl, 15–16 years, Essex)

Children also learn from widely debated ‘privacy buzz cases.’ For example, high-profile privacy breaches (such as Cambridge Analytica) or public discussions of new regulations (such as the European General Data Protection Regulation) are examples that even the youngest children brought up in their discussion of privacy:

> Facebook sold the information of their users to a different company who made things to put people off of voting for someone. (Boy, 11–12 years, Essex)

> Mark Zuckerberg, he’s always watching. (Boy, 15–16 years, Essex)

Legal and policy changes are harder to grasp than front-page privacy breaches, but their repercussions attract children’s attention as well. Children had noticed that they are asked about cookies on all the sites they visit, that notifications about changes to privacy policies of social media platforms had started to pop up, while their schools had sent letters home asking for consent for data collection. Such developments serve as learning opportunities for children, even though not all can follow the debates or fully understand the issues. Not integrating such ‘privacy buzz moments’ or new regulatory changes into children’s (formal or informal) digital literacy education seems like a wasted opportunity, especially when they are intrigued by the topics that everyone seems to be talking about, and that are affecting their daily online experiences.

However, left on their own, most children do not learn more complex digital skills or engage in the full spectrum of online opportunities (Livingstone, 2019). Data literary is not a competence which is easy to master and such knowledge is hard to come by without a scaffolded learning process. Hence, it is not surprising that, in spite of their active approach to learning, children have many gaps and misconceptions. Terms are misleading—why is it consent if you must agree to use the service? Why is it called deletion if nothing is really gone permanently? Policies are illegible to children because “there is quite weird language on purpose to trip you up” (girl, 13–14 years, London). It is perplexing to them why some apps request information that seems irrelevant to the services they provide, and children find it counterintuitive that companies want to keep data that quickly becomes outdated or that they know to be wrong because they have provided misleading information. At the same time, as we have seen, children are often trusting of companies, expecting them to protect the privacy of their customers, to collect data to improve the user experience and to follow the rules so as not to jeopardize their own reputations.

Trying to make sense of how the data ecology works, children create their own hypotheses, myths and resolutions, drawing on their familiar interpersonal experiences although these may be inappropriate to the circumstances. Notably, children find it hard to imagine why any company would be interested in their data and why this might have privacy implications, when they have ‘nothing to hide’:

> I just don’t think that what the ordinary everyday person does on the Internet is really that interesting to companies and even if they take data, I don’t think that anything bad will happen to me. (Girl, 13–14 years, London)

> I don’t really do any sensitive stuff on the Internet….Why would somebody want to track me down? (Boy, 11–12 years, London)

> I don’t see what they’d get out of it [selling my data], to be honest. (Girl, 15–16 years, Essex)

5.2. Can These Gaps Be Addressed by Media Literacy Education at School?

Formal education is an important source for learning about online privacy, be this as part of the curriculum on media education, computing, citizenship, or elsewhere. In our discussions, children often mentioned learning about different privacy issues—online contact, sharing information, privacy settings, cookies, or geolocation—in class or following teachers’ advice on how to avoid online risks. They also acquire practical technical skills in tasks ranging from easier ones like using email to much harder ones like learning a programming language. But how realistic is to expect that all gaps in children’s knowledge and skills related to data and privacy online can be addressed in educational settings?

Talking to children revealed many challenges and gaps in the current curriculum. Most of schools’ emphasis is on e-safety, including attention to interpersonal privacy and data given, but offering them little understanding of institutional or commercial data practices. We also found that children’s knowledge relates predominantly to their current or near future situation, but rarely encompasses the possible long-term consequences of their digital footprint for employment or further education. Yet, there are many things that children want to learn more about, extending beyond their interpersonal experience to encompass also how the Internet works and how their data flows.

Indeed, when we asked them what they want to learn, children quickly assembled a list of questions, many of which we could not ourselves answer with certainty. Children want to know where their data goes, who keeps it and why, for how long their data is stored, its use and with whom it is shared. They are puzzled by the bigger picture, asking about how the Internet works, who controls it and who makes decisions about the consequences of selling personal data. Many of their questions showed their desire to have more control over their privacy—how to change their data and digital footprint and how to have better privacy without having to stop using social media or other digital resources. Some seemingly naïve questions, like "What do they do with your face when you use facial recognition?" tap important issues about the future of datafication and the dangers arising from the endless surveillance possibilities of governments and corporations. Children are prepared to do the work to gain this knowledge and want schools and parents to step up to teach them about these issues, but they also want companies to make things easier for them to understand on their own. This seems to open up an opportunity for schools, given children's enthusiasm to learn more.

But these issues are not easy to teach about, and this would require further training of educators and updates to the school curriculum. Children and their teachers discussed the difficulties of keeping the curriculum up to date and sufficiently engaging:

> What about the people who still don't know how to send emails or anything like that? Because I still struggle with sending emails. Like, I just still….I can't get my head around it. (Girl, 13–14 years, Wales)

> We just get bored and don't listen. (Girl, 13–14 years, Essex)

> What they're trying to say is just, like, oh yes, don't do this, don't do that, don't do this. When it's, like, basically the whole point of that thing. (Girl, 13–14 years, Scotland)

Differences in the competence of children, even of the same age, can be quite pronounced, and these are likely to increase further as more privileged parents gain more knowledge and can support their children differentially. This can make teachers' task complicated, but also opens up possibilities for encouraging peer learning and makes the role of schools all the more important in improving equity in privacy and data literacy. In some of the schools we visited, we found that concerted efforts to offer a more comprehensive curriculum seem to show positive results, with children at some of the research locations appearing notably more knowledgeable than at others. Yet, even the most competent children struggle with some aspects of datafication, commercialization of personal information or data flows that are simply beyond their comprehension, and in many cases also beyond that of parents and educators.

In spite of the many challenges faced by digital literacy education at present, our research also demonstrates the unique position of schools as institutions tasked simultaneously with educating students and with managing their personal data. The trust that children and parents place in schools, the access that schools have to all children equally, and the fact that children spend years in school, means that schools have a rare opportunity to deploy their own data protection and management practices as a pedagogical strategy extended over real time and to teach children about privacy, the mechanics of data gathering and protection, and the rights and responsibilities associated with sustaining standards of transparency, security, fairness and data justice (Gangadharan & Niklas, 2019). In schools, therefore, the theory and practice of online privacy and data protection could be productively aligned, thereby offering children an example of best practice that would enable them to view the practices of other organizations critically where merited (Stoilova et al., 2019).

Arguably, however, regardless of how good their education is or becomes, children cannot be expected to fully comprehend and manage their data and privacy online in the current and ever-innovating digital environment. Children are trying to engage with an environment that is generally not designed with their interests or capacities in mind and that is fully comprehensible neither to children nor to many adults. Moreover, the design and operation of digital services continue to be largely 'age-blind,' without regard for whether the person in front of the screen is a minor, and to innovate in highly complex ways led by an incentive structure that rarely prioritizes human rights or ethics (Lievens et al., 2018). Hence, there are growing calls for educational efforts to be supported by greater regulation of the technology sector, including for legislation mandating privacy-by-design solutions (Barassi, 2019; Culver & Grizzle, 2017; Kidron et al., 2018; UNICEF, 2018; van der Hof, 2016).

6. Conclusions

The more children's lives become digital-by-default, the more the design and functioning of the digital environment matters, as do children's understanding of and capacity to manage their data and privacy online. Children are involved, one way or another, in all interpersonal, institutional and commercial privacy contexts, each with its own distinctive logic and outcomes. Our child-centred qualitative study of children's understanding of these contexts revealed that children primarily conceptualize privacy, including their own data online, in relation to interpersonal contexts. As expected, children are most familiar with the contexts where they play an active role in how their data is shared, rectified, used and removed. Significantly, they draw on this understanding to generalize about privacy and to guide their data protection tactics in other contexts.

Some aspects of how privacy works in institutional contexts are also familiar, but here children rely on existing regulations and build relationships of trust to manage their privacy. This accords them a fairly passive role within an environment where they are heavily monitored and regulated (Steeves & Regan, 2014) and are accorded little knowledge or choice. Children's expectation of agency, and their tendency to trust familiar institutions, make for a doubly problematic orientation towards data and privacy online in commercial contexts, leading to a mix of frustration, misapprehension and risk. Finally, children find the commercial domain perplexing and manage to grasp only some aspects of how it operates. Again, they have little choice but to adopt a fairly passive approach to privacy because of the choice architecture (Thaler, Sunstein, & Balz, 2013) of digital systems, which offers the user only superficial alternatives but no real ways to manage their privacy, while still benefiting from the services. This has important implications for digital literacy, media education and for child rights in a digital-by-default age (Lievens et al., 2018).

Struggling to make sense of how the data ecology works, children attempt to learn actively—trying out, searching and figuring things out on their own. Creating their own hypotheses and resolutions as a way of coping with a rapidly changing environment, children sometimes fall into the trap of misconceptions and have many competence gaps, particularly in institutional and commercial contexts. Insofar as education is part of the solution, these challenges, and the continued pace of technological innovation, raise the bar for children's digital literacy, which is the fastest-changing part of media literacy (Livingstone et al., 2020). At present, schools tend to teach a combination of e-safety and computer programming, but attention to the digital economy and its technological and business operations is rarely included in the computer science or media education curricula (Polizzi, 2020). Our findings suggest that children not only need better digital skills to manage their data and privacy online, but they also need a more comprehensive understanding of how the digital environment works—in terms of its technology, political economy, business and governance. This is challenging to teach, both because of its complexity and pace of change, and because the digital infrastructure of modern societies shares the character of all infrastructures—they are routine, taken-for-granted, noticed only when they break down (Lievrouw & Livingstone, 2009). Moreover, what is needed is a flexible educational approach that recognizes differences among children and promotes their understanding of their rights as digital citizens and data subjects. This should provide particularly for vulnerable or disadvantaged children, given the potential for abuses of sensitive data and for discrimination in relation to automated decision-making.

Not only do children need and want to play an active role in decision-making about online participation and privacy protection, but businesses, parents and the state have a shared responsibility to create a legible and transparent online environment where children have real choices and agency. Specifically, the technology industry needs to take greater steps to respect children's rights and well-being, including through supporting privacy-by-design, data justice and a platform duty of care (Lievens, et al., 2018; LSE Truth, Trust and Technology Commission, 2018; Lupton & Williamson, 2017). Also important is the need for stronger data protection regulation and enforcement. As the policy climate shifts to reconsider rebalancing the responsibility for managing privacy in a digital world between provider and consumer, along with redesigning services and developing accessible systems of redress, democratic politics requires that citizens' voices must be heard on their opinions and concerns. This applies to children as much as to adults, as stated in Article 12 of the UN Convention on the Rights of the Child (UN, 1989). At present, in most policy consultations on data and privacy online, the 'data subject' is treated as ageless, and there is little consultation with children or specific regulatory provision for children's data rights and the protection of their privacy (Livingstone, 2018). An exception is the recent introduction of the UK's Age-Appropriate Design Code, part of the 2018 Data Protection Act—itself based on a consultation with children among other stakeholder groups (Information Commissioner's Office, 2019; Revealing Reality, 2019).

In the societal effort to transcend the too-simple binary choice of education or regulation, it is important to hear children's voices, and to recognize their desire to exercise agency but not to face overwhelming risks in relation to the digital environment. While children wish to take responsibility for their own digital lives, this must rest in part on understanding, and in part on the design and operation of the digital environment: if the latter is opaque, highly technical and fast-changing, children's understanding (and that of the adults who support them) will continue to be challenged and their privacy at risk.

Acknowledgments

We thank the UK Information Commissioner's Office for funding this project, accessible at www.myprivacy.uk. We are also grateful to Julian Sefton-Green for the concept of 'digital-by-default.'

Conflict of Interests

The authors declare no conflict of interests.

References

Barassi, V. (2019). Datafied citizens in the age of coerced digital participation. *Sociological Research Online*, *24*(3), 414–429.

Bowler, L., Acker, A., Jeng, W., & Chi, Y. (2017). "It lives all around us": Aspects of data literacy in teen's lives. In S. Erdelez & N. K. Agarwal (Eds.), *Proceedings of the association for information science and technology* (pp. 27–35.) Hoboken, NJ: Wiley.

Buckingham, D. (2015). Defining digital literacy: What do young people need to know about digital media? *Nordic Journal of Digital Literacy*, *10*, 21–35.

Buitelaar, J. (2018). Child's best interest and informational self-determination: What the GDPR can learn from children's rights. *International Data Privacy Law*, *8*(4), 293–308.

Culver, S., & Grizzle, A. (2017). *Survey on privacy in media and information literacy with youth perspectives*. Paris: UNESCO.

Davis, K., & James, C. (2013). Tweens' conceptions of privacy online: Implications for educators. *Learning, Media and Technology*, *38*, 4–25.

Gangadharan, S., & Niklas, J. (2019). Decentering technology in discourse on discrimination. *Information, Communication & Society*, *22*(7), 882–899.

Information Commissioner's Office. (2019). *Consultation on age-appropriate design: Summary of responses*. Wilmslow: ICO. Retrieved from https://ico.org.uk/media/about-the-ico/consultations/aadc/2616996/summary-of-responses.pdf

Kidron, B., Evans, A., & Afia, J. (2018). *Disrupted childhood*. London: 5 Right Foundation. Retrieved from https://5rightsfoundation.com/uploads/5rights-disrupted-childhood-digital-version.pdf

Kumar, P., Naik, S., Devkar, U., Chetty, M., Clegg, T., & Vitak, J. (2017). No telling passcodes out because they're private. *Proceedings of the ACM on Human–Computer Interaction*, *1*, 1–21.

Laufer, R., & Wolfe, M. (1977). Privacy as a concept and a social Issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42.

Lievens, E., Livingstone, S., McLaughlin, S., O'Neill, B., & Verdoodt, V. (2018). Children's rights and digital technologies. In T. Liefaard & U. Kilkelly (Eds.), *International children's rights law* (pp. 1–27). Berlin: Springer.

Lievrouw, L., & Livingstone, S. (2009). Introduction. In L. Lievrouw & S. Livingstone (Eds.), *New media: Sage benchmarks in communication* (pp. xxi–xl). London: Sage.

Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications: The European Journal of Communication Research*, *39*(3), 283–303.

Livingstone, S. (2018). Children: A special case for privacy? *InterMedia*, *46*(2), 18–23.

Livingstone, S. (2019). Are the kids alright? *Intermedia*, *47*(3), 10–14.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2020). Data and privacy literacy: The role of the school in educating children in a datafied society. In D. Frau-Meigs (Ed.), *Handbook on media education research* (pp. 413–425). London: Wiley Blackwell.

LSE Truth, Trust and Technology Commission. (2018). *Tackling the information crisis: A policy framework for media system resilience*. London: London School of Economics and Political Science. Retrieved from http://www.lse.ac.uk/media-and-communications/truth-trust-and-technology-commission/The-report

Lupton, D., & Williamson, B. (2017). The datafied child. *New Media & Society*, *19*(5), 780–794.

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

Mascheroni, G. (2018). Researching datafied children as data citizens. *Journal of Children and Media*, *12*(4), 517–523.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences, 374*(2083), 1–17.

Murumaa-Mengel, M. (2015). Drawing the threat: A study on perceptions of the online pervert among Estonian high school students. *Young*, *23*, 1–18.

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

Pangrazio, L., & Selwyn, N. (2018). 'It's not like it's life or death or whatever': Young people's understandings of social media data. *Social Media and Society*, *4*(3), 1–9.

Petronio, S. (2002). *Boundaries of privacy: Dialects of disclosure*. New York, NY: SUNY Press.

Polizzi, G. (2020). Digital literacy and the national curriculum for England. *Computers & Education*, *152*, 1–13.

Revealing Reality. (2019). *Towards a better digital future*. Wilmslow: Information Commissioner's Office. Retrieved from https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf

Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media & Society*, *3*(1), 1–14.

Schou, J., & Svejgaard Pors, A. (2019). Digital by default? A qualitative study of exclusion in digitalised welfare. *Social Policy Administration*, *53*, 464–477.

Selwyn, N. (2019). What's the problem with learning analytics? *Journal of Learning Analytics*, *6*(3), 11–19.

Solove, D. J. (2015). The meaning and value of privacy. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 71–81). Cambridge: Cambridge University Press.

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313.

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

Thaler, R., Sunstein, C., & Balz, J. (2013). Choice architecture. In E. Shafir (Ed.), *The behavioral foundations of public policy* (pp. 428–439). Princeton, NJ: Princeton University Press.

UN. (1989). Convention on the rights of the child. New York, NY: UN. Retrieved from https://www.unhcr.org/uk/4aa76b319.pdf

UNICEF. (2018). *Children's online privacy and freedom of* *expression*. New York, NY: UNICEF.

van der Hof, S. (2016). I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal*, *34*(2), 409–445.

Westin, A. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Zuboff, S. (2019). *The age of surveillance capitalism*. London: Profile Books.

About the Authors

Mariya Stoilova is a Postdoctoral Researcher at the Department of Media and Communications, London School of Economics and Political Science. Her work falls at the intersection of child rights and digital technology, focusing particularly on the opportunities and risks of digital media use in the everyday lives of children and young people, data and privacy online, digital skills, and pathways to harm and well-being. Mariya's work incorporates multi-method evidence generation and cross-national comparative analyses. For projects and publications see here: https://www.lse.ac.uk/media-and-communications/people/research-staff/mariya-stoilova

Sonia Livingstone (FBA, OBE) is a Professor in the Department of Media and Communications, London School of Economics and Political Science. Her 20 books include *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives*. She directs the projects Children's Data and Privacy Online, and Global Kids Online (with UNICEF) and has advised the European Commission, European Parliament, Council of Europe, ITU, OECD and others on children's risks and rights in a digital age. See www.sonialivingstone.net

Rishita Nandagiri was a Research Assistant on the Children's Data and Privacy Online project. Her research focuses on gender and reproduction in low-and-middle-income countries. She is currently an ESRC Postdoctoral Fellow, Department of Methodology, London School of Economics.

COGITATIO

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 208–217
DOI: 10.17645/mac.v8i4.3247

Article

“The Kids Hate It, but We Love It!”: Parents’ Reviews of Circle

Davide Cino [1,*], Giovanna Mascheroni [1] and Ellen Wartella [2]

[1] Department of Communication and Performing Arts, Catholic University of the Sacred Heart, 20123 Milan, Italy;
E-Mails: davide.cino@unicatt.it (D.C.), giovanna.mascheroni@unicatt.it (G.M.)
[2] Department of Communication Studies, Northwestern University, Evanston, IL 60208, USA;
E-Mail: ellen-wartella@northwestern.edu

* Corresponding author

Submitted: 11 May 2020 | Accepted: 10 August 2020 | Published: 10 November 2020

Abstract

The contribution aims to present a critical analysis of Circle—a screen time management and parental control device—through the lens of parental mediation, children’s surveillance, and children’s rights to online participation. Circle promises to sell parents peace of mind by allowing them to monitor their children’s online activities. In order to investigate how parents themselves understand Circle, we conducted a quantitative and qualitative content analysis of a sample of 154 parental reviews about the device on Amazon and Searchman by parents of children from early childhood to adolescence, with respect to perceived advantages and disadvantages of the device, parenting styles, and (the absence of) children’s voice and agency. Results suggest an ambivalent relationship between parents and the device. Most reviews adhere to the dominant discourses on ‘screen time,’ framing children’s ‘intimate surveillance’ as a good parenting practice, and emphasize the need for the ‘responsible parents’ to manage their children’s online experiences with the aid of Circle. Others, in turn, criticize the device for failing to enable fine grained monitoring, while few reported the device could dismiss children’s voice and cause conflicts in the households. Overall, findings suggest that parental control devices may promote restrictive mediation styles hindering children’s voice and their exploratory and participatory agency online.

Keywords

children; Circle; parental mediation; privacy; surveillance

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

Mobile media are an integral part of family life today in the Global North. According to the Common Sense Census (Rideout, 2017), 98% of American households with offspring aged 0–8 hold at least one mobile device accounting for a third of children’s screen time, with the average child in that age range spending 48 minutes a day on it. Nationally representative data from over 16,000 8- to 18-year-olds in the U.S. found that by age 11.53% of children possess their own smartphones, with a rise to 69% by the time a child turns 12, with time spent on screen media for entertainment purposes ranging from 5 to 7 and a half hours a day (Rideout & Robb, 2019). Additionally, data from EU Kids Online report that among European children aged 9–16, 80% go online with a smartphone or mobile device, with the average child spending approximately 167 minutes a day connected (Smahel et al., 2020). Taken together, these studies suggest that using mobile devices is common practice for many children today in industrialized countries.

A peculiar characteristic of mobile media is their ubiquity, as users can access them ‘anywhere, anytime,’ crossing traditional boundaries of media usage within specific rooms in the domestic environment and contributing to “the geographical migration of technologies” in the household (Caron & Caronia, 2001, p. 43; Radesky, Schumacher, & Zuckerman, 2015). This means that media use and Internet access can become increasingly privatized experiences for children who live far from their parents' supervision, potentially fostering a pervasive and unsupervised use at every moment of the day and night. In this regard, survey findings, for example, show that the 39% of teens owning a mobile device keep it within reach when sleeping. Of these, the 70% check it within 30 minutes before falling asleep, while 51% tend to wake up at night to check social media, and 54% wake up because of a notification (Robb, 2019). Such ubiquity of mobile media in the life of youth seems to worry many parents of children from early childhood to adolescence (Lauricella et al., 2016; Rideout, 2017; Rideout & Robb, 2019), for traditional parental mediation strategies are hindered by smaller screens and more personal devices. A national-representative study of U.S. parents with children aged 8–18, for example, found that 53% of them fear their kids may develop some addiction to their screens, while 85% agree that monitoring children's media usage is important for their safety, and 67% believe that it is more important than respecting their privacy (Lauricella et al., 2016). As children's screen time has been framed as a social, yet private, problem calling for parents' responsibility in handling it, many tools have been developed in the past few years to help parents in this task. In this regard, Common Sense data report that 31% of parents use third-party tools to govern their children's device use, such as Internet filters, Net Nanny, and Circle (Lauricella et al., 2016). These findings are further supported by children themselves, as among over 16,000 youth from the abovementioned study from Rideout and Robb (2019), half of all tweens and a quarter of teens with a smartphone or a tablet stated their parents use some apps or other tools to monitor what they do and how much time they spend online.

On such basis, the present exploratory study seeks to investigate parents' perceptions of and experiences with parental control technological tools as means of parental mediation of children's technology use. As an example of these devices, we specifically focus on Circle, a small box that connects to the home network for parents to monitor and regulate children's Internet use from all devices in the house, promising "to make families' lives better, online and off" (MeetCircle, n.d.). According to the website, its features allow parents to: limit children's online activities by filtering contents, setting time limits and pause the navigation; check pattens of individual Internet usage, visited websites, and trace children's location; keep balance, by setting a bedtime for children's devices, scheduling off times from the Internet, and giving motivational rewards by granting extra time online to give kids a "little boost for good behavior" (MeetCircle, n.d.).

Drawing on a broader project on the domestication of parental control tools, here we report on a quantitative and qualitative content analysis of users' reviews of Circle posted on Amazon and Searchman in order to explore how parents understand and rate Circle within the household, with respect to parents' perceived advantages and disadvantages of the device, parenting styles, and (the absence of) children's voice and agency in the monitoring process.

2. Literature Review

2.1. Leisure Time, Screens, and Parental Accountability: What's New?

Media panics surrounding the relationship between children and the media have long historical roots, with every medium being cyclically considered a potential threat to moral order (Drotner, 1999), and worries about digital media use being a topical and daily source of dilemmas for many families in the digital age (Blum-Ross & Livingstone, 2020).

According to Furedi (2016), the emergence of commercial publishing during the 18th century and the increase in the number of books' readers led to the fear of a 'reading addiction' in terms of potential alienation of the consumers and, especially for the youth, copycat effects to emulate characters' behaviors and deeds. Similarly, the rise of penny newspapers in the 19th century spurred similar controversies, echoing concerns that came with every 20th century new medium in terms of their potential disruptive effects on children, from films to smartphones and tablets. On such bases, it has been argued that every medium has been accompanied by broader social discourses on its peculiar advantages and disadvantages, with society putting particular emphasis on parents as primarily responsible for their children's media-related opportunities while also protecting them from potential risks (Blum-Ross & Livingstone, 2016; Wartella & Jennings, 2000). This narrative contributed to a 'Jekyll-and-Hyde' phenomenon, where, on the one hand, parents receive social pressure to incorporate the media in the household in order for their children not to miss out on educational benefits, but on the other, they are invested with the burden of protecting their children's safety and wellbeing. Such an expectation is in line with the intensive parenting framework, according to which parents are to deterministically be deemed accountable for all of the functional or dysfunctional outcomes in their children's lives (Shirani, Henwood, & Coltart, 2012). When applying this risk-benefit ratio to govern media 'effects,' parents have been asked to focus both on the amount of time children spend using the medium, and on the effects of children's exposure to media content in terms of knowledge, values, and moral conducts (Caronia, 2010). In spite of policies aimed at controlling the access to, and the quality of media for children, society has historically framed parents as the primary gatekeepers for safeguarding children from media's potentially harmful effects.

Furthermore, as historical discourses on media tended to recognize their educational opportunities for kids (e.g., for school-related activities), questions of media governance have always paid particular attention to children's leisure time, where the media could be used by kids on their own mainly for entertainment purposes, against socially accepted expectations on how this free time should be spent (Wartella & Robb, 2008). Governing children's time with the media, though, progressively became a complicated task due to the growing privatization and individualization of media use in the household (Wartella & Jennings, 2000). Once again, same patterns of social worries and reactions have been seen with new mobile technologies (Wartella, 2019), where opportunities for privatization of media use reach a whole new level.

In light of broader social discourses framing parents as accountable to find private solutions to public 'problems' (i.e., children's relationship with media and its broader societal impacts), specific parental mediation strategies have been developed to govern (digital) media in the household. The next paragraph will build on that, specifically on how new technologies themselves—such as Circle—can be used to surveil children's relationship with mobile media.

2.2. Digital Parenting: Extending Parental Mediation and Parenting through Space and Time

Since most media use in childhood takes place at home (Lemish, 2015), as noted above, parents have always been called upon to regulate their children's relationship with the media by disciplining both time and content. The practices, values and norms through which parents attempt to regulate their children's use of media—for example, trying to find a balance between media use and outdoor activities or encouraging positive uses of technology—have been traditionally labelled as 'parental mediation.' Parental mediation materializes parents' attitudes and imaginaries—hopes and fears—towards digital media. However, parental mediation practices reflect more largely the overall parenting and childrearing cultures of each household (Clark, 2013). While the study of parental mediation started in relation to television (co-)viewing, research is in agreement in pointing out how digital media complicate parental mediation. First, as anticipated above, digital and mobile media favor further privatized access to and use of the Internet and technology, as opposed to shared activities of co-viewing and a communal family-centered media experience, which in turn hinders the simple transfer of traditional parental mediation strategies from television to digital media (Valkenburg, Krcmar, Peeters, & Marseille, 1999). Second, and most importantly, is the double-faced nature of digital media, that simultaneously represent both the object of parental concerns and their regulatory attempts, and resources for parenting through anxiety-reducing devices (Ribak, 2009). Indeed, digital parenting (Mascheroni, Ponte, & Jorge, 2018) indicates the profound incorporation and naturalization of digital tools in the everyday practices of parenting, including forms of remote parenting (Clark, 2013) and micro-coordination of family life, up to the emergent practices of transcendent parenting (Lim, 2020) and intimate surveillance (Leaver, 2017). Transcendent parenting refers to the mobile-based and online-based practices through which parents transcend physical distance, and the boundaries between online and offline interactions, in order to be always 'there' for their children. Mobile media and digital media, then, support an extension of parenting across space, by transcending the limits of physical proximity, and across time, enabling an intensive and timeless enactment of parenting and a continuous provision of care at a distance (Lim, 2020).

Newer technologies, like mobile media, online platforms, apps and wearable devices become then part of the household's moral economy (Silverstone & Hirsh, 1992), by being acquired, domesticated, adopted and made meaningful in the context of the relation of care between parents and their children in line with the house's moral values and parents' orientation on parenting and the role they (feel they) are supposed to play in order to manage the relationship between technology and the offspring. In this way, the monitoring of children's lives—including their biometrics and health—becomes normalized as a good parenting practice. While providing parents with feelings of empowerment for adopting a caring and responsive parenting style, such emergent forms of 'intimate surveillance' (Leaver, 2017) or 'caring dataveillance' (Lupton, in press) situate business models and logics—namely datafication and 'surveillance capitalism' (Zuboff, 2015)—at the very heart of the intimate relationship between parents and children. The ambivalence of digital and mobile media as tools for empowerment, anxiety-reduction, and control within the parent–child relationship, first noted in studies of mobile communication (Ribak, 2009), is now turned into an everyday dilemma for parents (Cino & Dalledonne Vandini, 2020). In fact, the digital surveillance of children through various technologies of datafication is aimed at ensuring children's safety on and offline, while actually putting children's rights to privacy, protection and participation at risk (Mascheroni, 2018).

3. Methodology

Informed by the abovementioned literature, the present article investigates parents' use of and opinions about Circle through a quantitative and qualitative content analysis (White & Marsh, 2006) of reviews posted on Amazon and Searchman. Our approach was informed by previous studies researching parents' appropriation of smart assistants like Alexa or pregnancy apps using the same platforms as sources of data collection (Barassi, 2017; Purington, Taft, Sannon, Bazarova, & Taylor, 2017). The rationale behind combining a quantitative and qualitative approach rests on our intention to both quantify basic descriptive information concerning how Circle is incorporated in the family environment, while also interpreting these reviews to consider how they may reflect or resist broader social discourses on parents, children, and the media (Mascheroni & Holloway, 2017). This exploratory research aims to provide the basis for further inquiry on the topic in order to take a first glance at Circle's integration in the household. To this end, we seek to answer the following research questions:

> RQ1: How do parents' reviews evaluate Circle as a (digital-)parenting tool in the household?
>
> RQ2: What types of parenting styles and parental mediation strategies, if at all, do these reviews reflect and how do they intertwine with broader social discourses on parents' media governance?

3.1. Data Collection

Data for this study were collected on the U.S. Searchman and Amazon reviews' section of Circle Home Plus, the currently available device which substituted the first generation of Circle with updated features (such as an upgraded hardware and a feature to monitor children's mobile device use even outside the home). As such, the reviews are reflective of American users' experiences with the latest generation of the device. After an initial screening of the reviews, a total of 154 posts were collected on December 2019, 11 of which were manually removed as under-detailed, for a final sample of 143 reviews (66% from Amazon and 34% from Searchman).

3.2. Data Analysis

Data were analyzed following a mixed inductive-deductive coding approach, where codes were either derived from the reviews or informed by specific theoretical concepts. After a preliminary analysis of the sample, the authors prepared a provisional codebook which was tested by two external coders. Following an initial training, the research assistants independently coded 20% of the sample, with Cohen's Kappa levels of agreement ranging from .71 to .92. Once disagreements were discussed and resolved, the sample was split in two parts, and each coder coded one.

Where available, coders coded for background variables in order to try to contextualize our findings. These include: authorship (with four codes being inductively derived from the reviews of parent, child, grandparent, and other—$\kappa = .90$), author's gender (female, male, or other—$\kappa = .83$), presence of author's age (present, not present, and if present specify—$\kappa = .92$), and presence of child's age (present, not present, and if present specify—$\kappa = .91$).

Four other variables were included in the coding scheme. First, the perceived advantages of the device. The coders coded for presence or absence of advantages reported in the review through a binary code ($\kappa = .81$). The list of advantages was inductively derived by the authors when creating the codebook. As advantages were not mutually exclusive, coders coded each pro with a binary code to indicate the presence or absence of that specific asset. Seven codes were used: easy setup, possibility to tailor the device to children of different ages, possibility to monitor different devices, setting online time limits, checking websites' history, filtering inappropriate contents, and preventing arguments. Levels of agreement ranged from .73 to .80.

Second, the perceived disadvantages of the device. Coders followed the same procedure as above, coding for presence or absence of disadvantages in the review ($\kappa = .84$). Nine codes were inductively developed: difficult setup, slows down the Internet, crashes often, not flexible enough (used when the device would filter too many contents, even 'appropriate' ones), not enough monitoring, privacy risks in terms of data clouds, easy to circumvent, compromises parent–child relationship, and causes conflicts. Levels of agreement ranged from .75 to .82.

Third, the parental mediation. In line with Livingstone and Byrne (2018) we understand parental mediation as the strategies adopted by parents to manage the relation between children and media. Following the authors, reviews were coded as reflecting either a form of 'restrictive mediation,' 'enabling mediation,' or 'neither.' The 'restrictive' code was applied when the reviews' orientation pointed towards "restricting or banning or…supervising" (Livingstone & Byrne, 2018, p. 23) certain online activities. The 'enabling' code was used when, in turn, reviews spoke for an orientation towards "undertaking active strategies such as talking to a child about what they do online or encouraging their activities" but also "activities that might seem restrictive (use of technical controls and parental monitoring)…so that positive uses of the Internet can be encouraged" (Livingstone & Byrne, 2018, p. 23). The 'neither' code was used when none of the previous codes was pertinent. Agreement was high ($\kappa = .79$). While many frameworks on parental mediation are available—generally based on active, restrictive, and co-using strategies (Livingstone & Helsper, 2008; Nathanson, 2001; Valkenburg, Piotrowski, Hermanns, & De Leeuw, 2013)—the one provided by Livingstone and Byrne (2018) and Livingstone et al. (2017) was particularly relevant here, since not only it clearly recognizes the use of parental monitoring devices (in line with the focus of this article), but also that such an use should be understood in situational and contextual terms, as parents' intentions may in fact be to enable their children's Internet experience instead of hindering it.

Fourth, the parental 'ethic' towards digital media. This variable was conceptualized following Clark's (2013) notion of 'ethic' as a complex set of principles helping parents adopt certain courses of action when it comes to managing digital media within the home. As such, reviews were coded as reflecting either an ethic 'of expressive empowerment,' of 'respectful connectedness' or ‘neither.’ Reviews were coded as ‘expressive empowerment’ when reflecting an orientation toward encouraging children’s media use and respecting their independence and privacy. The ‘respectful connectedness’ code was applied when reviews would speak for an orientation towards children’s use of technology that would respect parental authority. The ‘neither’ code was used when none of the other codes was pertinent. Agreement was substantial ($\kappa = .76$).

4. Findings

The first step of this analysis was to look for posters’ background information in order to better contextualize our findings, though this is not always feasible when working with natural online data. With respect to authorship, 67% of reviews were coded as authored by a parent, 4% by a grandparent, 2% by children. While contextual cues suggest that the remaining 27% of reviews were authored by parents as well (among the other reasons because Circle is specifically marketed as a parental device and targeted to parents), they were coded as ‘other’ since no explicit indications were present. Most of the time authors’ gender was not clear (51%). When it could be inferred by nicknames or pronouns used in the review, though, 25% of the reviews were coded as authored by a man, and 24% as authored by a woman. Authors’ age was never reported, while children’s age was only reported for 11 children, 7 of which were teenagers, 2 were pre-teens, and 2 primary schoolers. Below, we report on parents’ perceptions of Circle and parenting orientations and approaches to digital media in the household.

4.1. Posters’ Perceptions of Circle

Of all the reviews, 52% indicated at least a perceived advantage, while 72% at least a perceived disadvantage of Circle. In terms of advantages, 39% of reviewers appreciated the opportunity to set time limits to their children’s Internet use, followed by 35% who indicated as a positive asset the possibility to use Circle’s functionality with different devices. 34% liked the device for its ability to filter contents by limiting access to specific websites, 31% reported the device was overall easy to setup, another 31% appreciated the opportunity to check kids’ navigation history. Furthermore, 20% indicated as an advantage the ability to tailor the device’s functions according to children’s age (so to differentiate settings for older or younger siblings), and 10% reported Circle could help preventing arguments about Internet use. When it comes to disadvantages, in terms of technical problems, 27% of reviewers lament the device is not flexible enough, as when using functions like the contents’ filter. It would risk blocking not only websites parents found inappropriate, but also others they would have allowed their children to visit. 26% of reviewers reported the device was difficult to setup, with another 26% lamenting it would slow down the Internet speed, while 19% reported the device crashes often and needs to be restarted to function again. 18% of reviewers claimed Circle failed to offer enough monitoring, as different posters felt like they could not control their kids’ overall online experience, while 11% stated children could easily find a way to circumvent it. Only 5% of reviewers reported that using this device could compromise parent–child relationships, 4% thought it could cause conflicts within the household, and just 2% thought it may lead to privacy risks for the information the device could collect and store in the cloud.

4.2. Parenting Orientation and Approaches to Digital Media

Among the reviews analyzed, 73 made explicit reference to a specific mediation style, of which 89% were coded as ‘restrictive mediation’ and the remaining 11% as ‘enabling.’ With respect to the variable ‘parental ethic towards digital media,’ after excluding the entries coded as ‘neither,’ 55 reviews were left, of which 87% reflected an ethic of ‘respectful connectedness,’ while 13% an ethic of ‘expressive empowerment.’ A Chi-square analysis was run to investigate whether the two variables were related. Results suggest a significant association between the ethic of respectful connectedness with a restrictive mediation style and the ethic of expressive empowerment with an enabling mediation style, X^2 (1, $N = 55$) = 38.46, $p < .001$, $\phi = .83$.

The qualitative analysis of the reviews led to the emergence of two main parental figures associated with the abovementioned mediation styles and ethics towards digital media: the anxiety-reducing restrictive caregiver (as in Ribak, 2009) and the reflexively enabling caregiver. As we shall see, these social figures both reflect and resist broader social discourses on the relationships between parents, children, and the media, which also contribute to the construction of the child as a passive or agentive actor in the process.

4.2.1. The Anxiety-Reducing Restrictive Caregiver

Reviewers echoing a restrictive mediation style and an ethic of respectful connectedness generally expressed enthusiastic views towards the device, framing it as an ‘answer to prayers’ and a ‘must in every house’ and emphasizing its function of empowering parents in being ‘in control’ of their kids’ use of the Internet. These reviews stressed the asymmetrical role between parents and children, where the former has the right to decide whether and how the offspring can access the web while neglecting the latter’s voice in the process. This excerpt from a father’s personal communication exemplifies that:

> Kids not responding to you? Pause the Internet. I can pause everyone or select an individual person or device. This is helpful in our house….My kids don’t like

> Circle, but we feel more in control of their usage so it's a winner for us.

The words of this father are reflective of a recurrent dichotomy we found across reviews, which can be conceptualized as 'Parent > Child.' While children have traditionally been framed as savvy users of technologies who can deceive their parents when using media (Facer, 2012), these posters reclaimed their right of turning the tables on their offspring, building on the monitoring opportunity offered by Circle. A mother, for example, praised the device for its being 'life changing' and 'well worth every cent': "No more haggling with the kids over rules and enforcement. You can control everything. I needed something to limit my kids multitasking on our laptop when he was supposed to be doing homework. Success!"

Matters of 'control' were recurrent in our corpus of data with the ability not only to monitor, but also stop children's use of digital media making feel parents confident in this task. These agentive feelings contribute to what we call the construction of an empowered parent, who finds in Circle an ally to his/her parenting and an anxiety-reducing tool. The above-mentioned excerpt suggests that according to some the device would allow parents to avoid traditional discussions on media use, functioning as a 'deputy' caregiver. Such an idea was reinforced by posters who praised the device for allowing them to successfully ease the task of setting rules with their kids. An example of that was having children respect bedtime during schooldays, which was seen as a 'much more manageable' effort thanks to Circle. The following excerpt reports on a parent who stresses that. As using technology would prevent the offspring from respecting bedtime rules, the device allowed to enforce this family's policy by tackling the problem at its root:

> I could not stand constantly telling my children to get off the computer and then arguing with them, 'just 5 more minutes.' Now at bedtime, Circle just turns off the Internet. Much better than my nightly attempts to pry them off. If they want more time, they have to come to me and ask….Unfortunately, we still have to do some parenting.

Overall, Circle was framed as a needed solution to deal with parenting challenges that these posters were no longer able to face through mediation strategies involving dialogue and authoritative rules with their kids. Conversely, the possibility to turn the Internet off and on whenever they wanted, led some parents to embrace a 'behaviorist' approach where allowing more or less time online could be used either as a positive reinforcement or a punishment. A poster, for example, stressed she appreciates the ability to "monitor each device and adjust rewards or punishments accordingly" in terms of additional or less time online, or—as in the words of another parent—to "give rewards like more time online when they do their chores."

Apart from parents' right to set rules limiting screen time, many posters emphasized the importance of monitoring kids' online activities and the contents they interact with on the Internet as a necessary strategy in line with their role of 'good' caregivers, stressing the need to protect children from online dangers within the "repertoire of official reasons" (Caron & Caronia, 2001, p. 44) for adopting Circle. This was evident in many reviews taking a moral stance towards the use of the device which was described as 'amazing for a family,' for it allows to "keep children safe and their screen time to the right amount" while giving parents peace of mind with respect to "the contents they come across often" and, as in the words of this mother, "sleep at night knowing that my kids are being safe online." Again, these example shows how Circle is discursively constructed as an anxiety-reducing device, which relieves parents from the burden of protecting children from exposure to online risks.

The topics of online safety and the 'right' amount of screen time work here as moral imperatives to justify one's parenting strategy as 'good' and 'caring.' The technologically enabled restrictions and surveillance through Circle are legitimized as a practice of care. The following excerpt exemplifies this ethical duty referring to the alleged news stories about "naïve" children victim of the web, providing a morally oriented rationale for making the adoption of Circle socially acceptable and even desirable for a caregiver:

> Each day we are bombarded with terrifying stories in the news about how children are exploited online just because they are naive, and with Circle Home Plus I am able to keep an eye on their online activity….I find this to be a wonderful tool for protecting your children.

Overall, the reviews supporting an 'anxiety-reducing and restrictive caregiver' discourse converged in disregarding children's rights to have a voice when making decisions about their online access and use. Parents who are enthusiastic about Circle seemingly found in the device a precious ally to enact forms of restrictive- yet morally informed-mediation while reinforcing an ethic of respectful connectedness that emphasizes parental authority when using the media within and outside the domestic walls.

4.2.2. The Reflexively Enabling Caregiver

Although strikingly lower in number, reviewers echoing an enabling mediation style and an ethic of expressive empowerment took a more critical stance towards the device, framing it either as a complementary means which helped some parents "to surface a lot of deeper conversations with kids about why and how we all use the Internet," or as a tool to avoid conflicts in the family environment. While slightly counterintuitive at first sight—if anything because one may wonder why an enabling caregiver may want to use this device—such a parental figure is theoretically in line with the enabling mediation style highlighted by Livingstone and Byrne (2018) and Livingstone et al. (2017) where seemingly restrictive technologically-supported strategies, such as adopting forms of technical controls, are not intentionally aimed at preventing children from using the Internet on their own. Rather, by ensuring that children's exposure to inappropriate content is minimized, technology restrictions are adopted within parental mediation strategies aimed at encouraging 'positive' and 'constructive' use of the medium, and promoting children's autonomous exploration of the Internet. Moreover, the device is appropriated as an intermediator between the child's online experience and the parent's mediating role, so as to minimize parents' supervision and control. The following excerpt offers some insights on how Circle can be incorporated in the family life while still respecting children's rights to online participation and privacy:

> We're involved parents who understand the benefits of video and the Internet but also recognize the existence of inappropriate content for our kids' ages and fact that it could become 'all consuming.' We don't want to eliminate screen time altogether but simply want to help manage our kids' overall consumption. So far Circle Home Plus offers the best solution we've found to manage online access in the house.

In the words of this parent, while children's right to go online should be safeguarded, Circle could help managing this experience to promote a 'healthier' approach to the Internet. This was also evident in the words of another poster who claimed that children themselves appreciated the role of the device for its being incorporated within a broader framework of family rules and conversations about Internet use that helped providing structure to their relationship with digital media. As this father states:

> Circle paved the way for conversations when I've seen excessive use of certain social media/websites/video streaming. The older teens have actually appreciated having limits and bedtimes/off-times to allow them play-time/break-time on their phones without the stress of being sucked in and losing hours of study or sleep time.

On the other hand, few reviewers denounced the fact that using Circle could dismiss children's voice in the process, causing conflicts in the households, and warning parents to "be ready for some major complaints and very unhappy kids." A parent, in particular, claimed: "If you want to torment your children, purchase this app and watch their hopes and dreams be flushed down the toilet," alluding to a possible decay in terms of children's trust towards their parents and overall wellbeing. Such a view was interestingly reinforced by a poster who was allegedly a child reviewing Circle as a tool limiting children's ability to explore the Internet on their own, denouncing the loss of privacy and overall unhappiness this caused him/her:

> I used to feel happy with what little privacy and Internet time I had but you made the little into none. If I could have rated a 5 stars then I would have. Now I feel that I have no privacy. Thanks for ruining my life!

All in all, this corpus of reviews framed the child as an active actor with the right of reclaiming agency against the backdrop of restrictive mediation strategies.

5. Discussions and Concluding Remarks: Empowering Parents, Disempowering Kids?

Taken together, our findings show that parents who choose to adopt Circle broadly adhere to the hegemonic discourses on children online, reinforcing the polarized identities of youth as 'vulnerable victims' and adults as 'protectors' (Facer, 2012). Circle offers a solution in line with the idea that in order to keep children safe from risks, their participation online should be restricted and controlled through strategies of 'helicopter' parenting (Clark, 2013). The alignment of parental imaginaries and practices with hegemonic discourses on children and media is also reflected in the recurrent preoccupation with the amount, more than the nature, of screen time (Blum-Ross & Livingstone, 2018). Parents who share their views on Circle appear to have fully incorporated the dominant advice on screen time, that suggest regulating the use of media mainly, if not exclusively, with time limits. Moreover, the analysis confirms parents' ambivalent attitudes towards technologies, which are perceived as both solutions to reduce parental anxiety and provide temporary relief from intensive parenting, and simultaneously as threats to parental authority and children's safety. This explains why most reviews are suggestive of a parenting style and childrearing culture that responds to online risks through an ethic of respectful connectedness (Clark, 2013). However, anticipating risks online is not straightforward, as opportunities and risks are positively correlated. Limiting children's time on the Internet through restrictive mediation is associated with lower skills, lower opportunities, and lower exposure to online risks, but greater vulnerability to the harmful consequences of online problematic experiences, since lacking experience with the Internet is associated with lower abilities to cope with situations where risks translate into harm (Livingstone & Helsper, 2010; Livingstone, Mascheroni, & Staksrud, 2018).

Nonetheless, the analysis offers a more varied portrait of parents adopting technological restrictions such as Circle, revealing that reviewers' understanding of the device speaks for different levels of consideration for children's agency. Indeed, the adoption of technical restrictions can take place within a repertoire of enabling strategies in contexts where parents struggle to find a balance between hopes for a digital future (Blum-Ross & Livingstone, 2018), concerns for online risks, and anxieties over societal pressure on parents, positioned as the only gatekeepers to children's wellbeing and safety.

In line with recursive historical trends of parental worries about media (Wartella & Jennings, 2001), these reviews suggest that Circle can help parents face "the geographical migration of technologies" in the household (Caron & Caronia, 2001, p. 43). Whether the child will be framed as an active or passive actor in the process, though, depends first and foremost on parents' intentionality, which may reinforce or resist broader discourses on parental mediation. Thus, Circle's adoption needs to be understood as a situated interactional process taking into account not only the device itself but also the actors' context and background.

This study was limited in nature and scope, relying only on natural data providing little demographic information, and a relatively small sample of reviews reflecting North American perspectives on the matter that may differ in other countries. Additionally, being a parent who uses a device such as Circle suggests some sort media literacy and technological skills, and in general suggests an enhanced level of concern and involvement with children's media-related experiences. This and the fact that these parents also went online to provide their feedback on the device gives the idea of an 'elite' sample of reviewers, whose experiences and opinions should be understood situationally in relation to this study. Future research, though, can be informed by our findings to better investigate how the incorporation of devices like Circle impacts on family dynamics and children's wellbeing, triangulating these results using other approaches that would help better contextualize them. Furthermore, researchers can investigate whether and how the unprecedent challenges caused by the Covid-19 pandemic shaped parents' perceptions of and use of such devices: In a context where screen time is required for children to attend classes, do their homework, and connect with family members and friends, how do matters of time spent with technology evolve and what role may devices like Circle play in family life? Last but definitely not least, future inquiry on the topic should actively include children's voices in the research process, in order to promote a multipart conversation and better consider how devices thought for empowering parents may, depending on their use, end up disempowering children.

Acknowledgments

The authors wish to thank research assistants Erica Demmi and Silvia Mirone, students at the University of Milan-Bicocca, for coding the database and providing insightful feedback throughout the data analysis process.

Conflict of Interests

The authors declare no conflict of interests.

References

Barassi, V. (2017). BabyVeillance? Expecting parents, online surveillance and the cultural specificity of pregnancy apps. *Social Media + Society*, *3*(2), 1–10.

Blum-Ross, A., & Livingstone, S. (2016). *Families and screen time: Current advice and emerging research* (Media Policy Brief 17). London: London School of Economics and Political Science.

Blum-Ross, A., & Livingstone, S. (2018). The trouble with "screen time" rules. In G. Mascheroni, C. Ponte, & A. Jorge (Eds.), *Digital parenting: The challenges for families in the digital age* (pp. 209–218). Gothenburg: Nordicom Clearinghouse Yearbook.

Blum-Ross, A., & Livingstone, S. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. New York, NY: Oxford University Press.

Caron, A. H., & Caronia, L. (2001). Active users and active objects: The mutual construction of families and communication technologies. *Convergence*, *7*(3), 38–61.

Caronia, L. (2010). The family's governance of children's media consumption as a moral arena: Theoretical framework, methodology and first results of a study. *RPD: Journal of Theories and Research in Education*, *5*(1), 1–20.

Cino, D., & Dalledonne Vandini, C. (2020). "Why does a teacher feel the need to post my kid?": Parents and teachers constructing morally acceptable boundaries of children's social media presence. *International Journal of Communication*, *14*, 1153–1172.

Clark, L. S. (2013). *The parent app: Understanding families in the digital age*. Oxford: Oxford University Press.

Drotner, K. (1999). Dangerous media? Panic discourses and dilemmas of modernity. *Paedagogica Historica*, *35*(3), 593–619.

Facer, K. (2012). After the moral panic? Reframing the debate about child safety online. *Discourse: Studies in the Cultural Politics of Education*, *33*(3), 397–413.

Furedi, F. (2016). Moral panic and reading: Early elite anxieties about the media effect. *Cultural Sociology*, *10*(4), 523–537.

Lauricella, A. R., Cingel, D. P., Beaudoin-Ryan, L., Robb, M. B., Saphir, M., & Wartella, E. A. (2016). *The common sense census: Plugged-in parents of tweens and teens*. San Francisco, CA: Common Sense Media.

Leaver, T. (2017). Intimate surveillance: Normalizing parental monitoring and mediation of infants online. *Social Media + Society, 3*(2). https://doi.org/10.1177/2056305117707192

Lemish, D. (2015). *Children and media: A global perspective*. Chichester: Wiley.

Lim, S. S. (2020). *Transcendent parenting: Raising chil-*

dren in the digital age. Oxford: Oxford University Press.

Livingstone, S., & Byrne, J. (2018). Parenting in the digital age: The challenges of parental responsibility. In G. Mascheroni, C. Ponte, & A. Jorge (Eds.), *Digital parenting: The challenges for families in the digital age* (pp. 209–218). Gothenburg: Nordicom, The Clearinghouse Yearbook.

Livingstone, S., & Helsper, E. (2008). Parental mediation of children's Internet use. *Journal of Broadcasting & Electronic Media*, *52*(4), 581–599.

Livingstone, S., & Helsper, E. (2010). Balancing opportunities and risks in teenagers' use of the Internet: The role of online skills and Internet self-efficacy. *New Media & Society*, *12*(2), 309–329.

Livingstone, S., Mascheroni, G., & Staksrud, E. (2018). European research on children's Internet use: Assessing the past and anticipating the future. *New Media & Society*, *20*(3), 1103–1122.

Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, *67*(1), 82–105.

Lupton, D. (in press). Caring dataveillance: Women's use of apps to monitor pregnancy and children. In L. Green, D. Holloway, K. Stevenson, L. Haddon, & T. Leaver (Eds.), *The Routledge companion to digital media and children*. London: Routledge.

Mascheroni, G. (2018). Researching datafied children as data citizens. *Journal of Children and Media*, *12*(4), 517–523.

Mascheroni, G., & Holloway, D. (Eds.). (2017). *The Internet of toys: A report on media and social discourses around young children and IoToys*. DigiLitEY.

Mascheroni, G., Ponte, C., & Jorge, A. (Eds.). (2018) *Digital parenting: The challenges for families in the digital age*. Gothenburg: Nordicom, The Clearinghouse Yearbook.

MeetCircle (n.d.). About Circle. *MeetCircle*. Retrieved from https://meetcircle.com/about

Nathanson, A. I. (2001). Parent and child perspectives on the presence and meaning of parental television mediation. *Journal of Broadcasting & Electronic Media*, *45*(2), 201–220.

Purington, A., Taft, J. G., Sannon, S., Bazarova, N. N., & Taylor, S. H. (2017). "Alexa is my new BFF" social roles, user satisfaction, and personification of the Amazon Echo. In G. Mark & S. Fussel (Eds.), *Proceedings of the 2017 CHI conference extended abstracts on human factors in computing systems* (pp. 2853–2859). New York, NY: Association for Computing Machinery.

Radesky, J. S., Schumacher, J., & Zuckerman, B. (2015). Mobile and interactive media use by young children: The good, the bad, and the unknown. *Pediatrics*, *135*(1), 1–3.

Ribak, R. (2009). Remote control, umbilical cord and beyond: The mobile phone as a transitional object. *British Journal of Developmental Psychology*, *27*(1), 183–196.

Rideout, V. (2017). *The common sense census: Media use by kids age zero to eight*. San Francisco, CA: Common Sense Media.

Rideout, V., & Robb, M. B. (2019). *The common sense census: Media use by tweens and teens, 2019*. San Francisco, CA: Common Sense Media.

Robb, M. B. (2019). *The new normal: Parents, teens, screens, and sleep in the United States*. San Francisco, CA: Common Sense Media.

Silverstone, R., & Hirsh, E. (1992). *Consuming technologies: Media and information in domestic space*. London: Routledge.

Shirani, F., Henwood, K., & Coltart, C. (2012). Meeting the challenges of intensive parenting culture: Gender, risk management and the moral parent. *Sociology*, *46*(1), 25–40.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., . . . Hasebrink, U. (2020). *EU kids online 2020: Survey results from 19 countries*. London: London School of Economics and Political Science.

Valkenburg, P., Krcmar, M., Peeters, A., & Marseille, N. (1999). Developing a scale to assess three styles of television mediation: Instructive mediation, restrictive mediation, and social coviewing. *Journal of Broadcasting & Electronic Media*, *43*(1), 52–67.

Valkenburg, P. M., Piotrowski, J. T., Hermanns, J., & De Leeuw, R. (2013). Developing and validating the perceived parental media mediation scale: A self-determination perspective. *Human Communication Research*, *39*(4), 445–469.

Wartella, E. (2019). Smartphones and tablets and kids: Oh my, oh my. In C. Donohue (Ed.), *Exploring key issues in early childhood and technology: Evolving perspectives and innovative approaches* (pp. 27–31). London: Routledge.

Wartella, E., & Jennings, N. (2000). Children and computers: New technology, old concerns. *The Future of Children*, *10*(2), 31–43.

Wartella, E., & Jennings, N. (2001). New members of the family: The digital revolution in the home. *Journal of Family Communication*, *1*(1), 59–69.

Wartella, E., & Robb, M. (2008). Historical and recurring concerns about children's use of the mass media. In S. L. Calvert & B. J. Wilson (Eds.), *The handbook of children, media, and development* (pp. 7–26). Hoboken, NJ: Blackwell Publishing.

White, M. D., & Marsh, E. E. (2006). Content analysis: A flexible methodology. *Library Trends*, *55*(1), 22–45.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

About the Authors

Davide Cino is a PhD Candidate in Education in Contemporary Society at the University of Milan-Bicocca. He is also appointed as a Research Associate at the Catholic University of the Sacred Heart, Milan, and a member of the Center on Media and Human Development at Northwestern University. His research interests include children's online experience and presence, digital parenting, and digital skills.

Giovanna Mascheroni (PhD) is an Associate Professor of Sociology of Media and Communications in the Department of Communication, Catholic University of Milan. She is part of the management team of EU Kids Online, and member of the Executive board and WP leader in the H2020 project ySKILLS. Her work focuses on the social shaping and the social consequences of the Internet, mobile media and Internet of Things and Toys for children and young people.

Ellen Wartella studies the role of media and technology in children's health and development. She is particularly interested in addressing public policy questions about children's use of media and technology. She is the Al-Thani Professor of Communication Studies, Chair of the Department of Communication Studies and Director of the Center on Media and Human Development at Northwestern University. She also holds appointments in Northwestern's School of Medicine, Department of Psychology and School of Education and Social Policy.

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 218–228
DOI: 10.17645/mac.v8i4.3350

Article

Privacy and Digital Data of Children with Disabilities: Scenes from Social Media Sharenting

Gerard Goggin [1,]* and Katie Ellis [2]

[1] Wee Kim Wee School of Information and Communication, Nanyang Technological University, 637718, Singapore; E-Mail: gerard.goggin@ntu.edu.sg
[2] Centre for Culture & Technology, Curtin University, Perth, WA 6845, Australia. E-Mail: katie.ellis@curtin.edu.au

* Corresponding author

Submitted: 15 June 2020 | Accepted: 4 September 2020 | Published: 10 November 2020

Abstract
Children with disabilities have been an overlooked group in the debates on privacy and data management, and the emergence of discourses on responsibilization. In this article, we offer a preliminary overview, conceptualization, and reflection on children with disabilities, their experiences and perspectives in relation to privacy and data when it comes to existing and emergent digital technology. To give a sense of the issues at play, we provide a brief case study of "sharenting" on social media platform (that is, sharing by parents of images and information about their children with disabilities). We conclude with suggestions for the research and policy agenda in this important yet neglected area.

Keywords
accessibility; children with disabilities; data rights; disability rights; Internet rights; privacy

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

Debate on privacy and data management, and the emergence of discourses such as responsibilization, has grown considerably in response to recent developments in digital technologies.

Activists, policy actors, scholars, children's allies, and others have pointed out the high stakes for children in the transforming digital environment—and argued for the importance of children's voices to be heard, listened to, and acted upon, in order for issues of privacy, data, surveillance, and so on, to be better understood and addressed (Livingstone & Third, 2017). There has been important work on privacy and children, and an acknowledgement that this is only the 'tip of the iceberg,' as this thematic issue underscores, in relation to children's perspectives, experiences, and voices.

An especially overlooked group in this regard are children with disabilities (Ellis, Goggin, & Kent, in press; Jordan & Prendella, 2019). While significant efforts have been made to bring attention to and address issues they face, and to support their participation in shaping digital technologies and policies, they remain notably under-represented in the various forums, institutions, corporate and policy arena. This situation has profound consequences, as Sonia Livingstone and Amanda Third underscore:

> The persistent exclusion of children living with disability illustrates a host of challenges associated with intersectionality online as offline. Such challenges are particularly acute online because of the hitherto lack of flexibility or contingency in the regulation of digital resources and infrastructure by comparison with the nuanced possibilities for shaping social norms and opportunity structures offline. (Livingstone & Third, 2017, p. 665)

Hence the importance of the moves to put children on the wider agenda of disability human rights as well as disability research. Also, the significance in the past two-plus decades of children with disabilities being recognized as an important part of the burgeoning area of children's rights, especially rights in relation to digital societies (Alper & Goggin, 2017; Livingstone & Third, 2017).

Consider, for instance, the overlap between the rights set out in both the 1989 UN Convention on the Rights of the Child (CRC) and the 2006 UN Convention on the Rights of Persons with Disabilities (CRPD; Alper & Goggin, 2017). The CRC was the first human rights treaty to dedicate an article to the rights of persons with disabilities (CRC, 1989, Article 23). For its part, the CRPD includes a standalone article on children with disabilities (CRPD, 2006, Article 7), the mainstreaming of children's rights via specific amendments (Schulze, 2010), and the inclusion of a number of child-specific issues such as birth registration, the right of children to family life rather than placement in institutions, and the right to play (Lansdown, 2014). The CRPD also includes a number of articles stipulating accessibility and inclusive design of digital technology, in particular—something that for the past fifteen years has been a touchstone for gauging progress on the wider global achievement of disability equality and rights.

There are a range of reasons why privacy and data in relation to digital media technologies stand to be just as or even more important for children with disabilities. Consider, for instance, the wide ranging efforts to specifically design and deploy many mobile technologies and apps to address specific requirements of a diverse range of children with disabilities; let alone the many ways in which children with disabilities access and rely upon a wide range of digital content, formats, and platforms to undertake many aspects of their daily home. Most of these technologies are underpinned by data collection and use, often gathering information from a range of inputs and interfaces (touch, voice, bodily and environment moment sensors, as well as traditional and new forms of user-generated content).

As yet we have little research that charts and theorizes these experiences and issues—let alone work by and with children with disabilities, as well as work that discusses the complex issues of voice and listening (cultural, social, and political) at play in emerging technologies, digital cultures, and platforms.

Accordingly, in this article, we offer a preliminary overview, conceptualization, and reflection on children with disabilities, their experiences and perspectives in relation to privacy and data when it comes to existing and emergent digital technology. To give a sense of the issues at play, we provide a brief case study of 'sharenting' on social media platform (that is, sharing by parents of images and information about their children with disabilities). We conclude with suggestions for the research and policy agenda in this important yet neglected area.

2. Children with Disabilities, Privacy, and Data

As it has been redefined in the past two decades, disability is now understood as a social, political, cultural, and rights-based matter, rather than some kind of biomedical condition or charity issue (Campbell, 2009; Goodley, Lawthom, Liddiard, & Runswick-Cole, 2019; Shakespeare, 2018).

For example, in accounts such as the social model approach, which developed from UK activists and disability researchers from the 1970s onwards (Oliver, 2013), disability is understood as the way that society responds to the realities of living life with impairments. According to proponents of the social model, people are disabled by their environment, by oppressive social relations and situations, rather than by the diversity of impairment and disabilities, which are part of what it is to be human and live in the world. Ideas, understandings, economies, and cultures, including technological systems, remain deeply shaped by problematic attitudes and stereotypes of disability, which are the correlates of the unjust, inequitable social arrangements that, while powerfully challenged in recent years, still persist and are unconsciously and deliberately reproduced (Beckett & Campbell, 2015). As part of this rich movement of disability activism, art, media, and research, there is now a significant, fast emerging body of work on media, technology, and disability (Alper, 2017; Ellcessor & Kirkpatrick, 2017; Ellis, Goggin, Haller, & Curtis, 2020; Lazar & Stein, 2017; Roulstone, 2016).

When it comes to children with disabilities and media specifically, the picture is less clear. In disability research, there is a body of rich research on experiences and perspectives of children with disabilities across a number of areas from health to media and cultural production, including accounts in their own voices (Ajodhia-Andrew, 2016; Foley et al., 2012; Runswick-Cole, Curran, & Liddiard, 2018). There is considerable work on inclusive research, and approaches to co-researching and collaborative research with children with disabilities (see, for instance, Liddiard et al., 2019). From the direction of children media's research (Alper, 2014) and especially recent research on Internet and digital rights of children, there are significant examples of research co-conceived and conducted with children aiming to support their independency, lived experiences, and ideas (see, for example, Benjamin-Thomas et al., 2019). As yet, however, there is little cross-over in terms of specific research on privacy and data issues and perspectives pertaining to and generated by children with disabilities. Given this gap, it is useful to return to some fundamental considerations about privacy and data, and the specific ways they unfold in relation to disability.

There is a longstanding discussion over diverse areas that affect people with disabilities (Montague, 1993). As Jasmine E. Harris puts it:

> Privacy and disability have an odd relationship. States, communities, and families, sometimes forcibly, have

> hidden people with disabilities from public view and engagement. In the shadow of a history of forced isolation and as a way of managing the stigma of disability, people with disabilities have, at times, rejected their public identity as disabled. (Harris, 2020, p. 159)

Key starting points include: the complex and important fundamental issues of an individual's personal information about their disability status; what meanings and contexts of disability are in relation to privacy and data; and what kinds of control and rights people with disabilities should be accorded and be able to exercise—in relation to what kinds of technologies. As Harris encapsulates it:

> While some people may explicitly deny disability identity for a host of legitimate reasons, more often, people with disabilities capable of "passing" choose to move in the world without disclosing their disability identity even when disclosure can lead to greater access to services, accommodations, or other benefits. At other times, people capable of passing who wish to disclose are discouraged and, at times, prevented from disclosing. (Harris, 2020, p. 159)

To give an example, in universities and schools across many jurisdictions, students with disabilities need to disclose their 'official' disability status, or 'register' as a student with disabilities (and be acknowledged as such) before they can receive 'accommodations.' Of course, this means that students with disabilities are registered and tracked by such educational systems—a part of a wider 'governmentality' of disability (Tremain, 2015). This also raises questions of so-called 'invisible disabilities,' not officially recognized or credited as triggering institutional responses and management. Also the question of the burden of inclusive education often rests on people with disabilities needing to declare disability status, rather than schools or universities ensuring inclusive, accessible environments, teaching, learning, and full membership of educational communities, as a matter of course (Price, 2011; Whitburn & Plows, 2017). Information regarding someone's disability is an issue widely seen as requiring confidentiality and raising privacy issues when it comes to employment and work (Twomey, 2010).

The visibilities, roles, and meanings of disability in the public sphere have been historically complex and often closely associated with the oppressions of disablism and ableism (Hadley, 2014; Iarskaia-Smirnova, 2020; Schweik, 2009). In turn, disability in the private sphere has been subject to other kinds of issues and modes of regulation (Priestley & Shah, 2011). Thus, the "privateness" and "publicness" of disability is a fraught and shifting area, along with other realignments of public and private life especially new forms of 'mediated visibility' key to constituting the public sphere now, amounting to what J. B. Thompson called a decade ago, 'mediated publicness' (Thompson, 2011, p. 56). Here the issues concerning privacy and data facing people with disabilities can be seen to flow into a larger set of issues about visibility, recognition (Maia, 2014), justice, voice (Couldry, 2010), and listening (Goggin, 2009).

This situation also may lead to some potential contradictions between advancing disability justice and rights, and older notions of disability privacy. Still we face well-founded fears that disclosure or communication regarding disability in relation to one's self—like sexuality or gender—would be a disadvantage, and lead to potential discrimination or disadvantage. Hence Jasmine Harris argues for a more "publicity-oriented approach to disability, particularly given the success of other social movements with this strategy," rather than relying upon "privacy and nondisclosure of disability status" (Harris, 2020, p. 170). She feels a discomfort with the latter, which she sees as a well-entrenched strategy that she feels construes privacy in a way that "undermines the very values disability rights law seeks to develop: the right to live in the world" (Harris, 2020, p. 170).

This kind of typical framing of disability and privacy is a main reason why this area remains extremely underexplored. Yet such investigation and discussion is urgent, given the intense societies' reliance on digital technologies with the issues they pose for privacy and data, as well as mediated publicness. As McRae, Ellis, Kent, and Locke (2020) point out, people with disabilities have particularly important and acute experiences, affordances, and perspectives on evolving privacy and data issues associated with digital technologies, and the mixed feelings many users have:

> This unease becomes acute when considering people with disability for whom technology and digital interfaces have become an essential and liberating part of the everyday. The ways in which these individuals form a node of and for a radical and reflexive engagement with privacy and consent, technology and society, and anonymity and visibility offer evocative terrain for consideration. (McRae et al., 2020, p. 423)

For instance, issues of control and consent when it comes to data have been in many ways anticipated by everyday digital life contexts of people with disabilities:

> People with disability monitor the boundaries between technology, consent, and privacy. Many of the privacy concerns currently being navigated by users of social media have been consciously engaged by people with disabilities who utilize assistive technologies, participate in cutting edge medical treatments or deal regularly with the medical industry, and who manage day-to-day intrusions upon their selfhood from inquiring gazes and invasive questions about their daily lives. (McRae et al., 2020, pp. 423–424)

So the kinds of considerations and desirata in understanding the 'contextual integrity' that Helen

Nissenbaum famously put at the centre of her influential concept of privacy (Nissenbaum, 2004, 2011) when it comes to people with disabilities. Such issues are all the more obscure and in need of discussion when it comes to children with disabilities. We will turn to this now, but very much having in mind the ethical, philosophical, and political trajectory that Harris marks out. That is, how we can understand privacy for children with disabilities that advances their rights to "live in the world," and adequately captures their valid "ways of being in the world" (Garland-Thomson, 2017, p. 133).

So, what are the kinds of privacy and data issues that are faced by children with disabilities in relation to digital technologies?

Privacy conditions, practices, and claims of children with disabilities in relation to their personal information and data certainly are strongly influenced by the shared conditions of digital infrastructures at present. These are the concerns widely raised by citizens, policymakers, and researchers alike, especially in relation to the affordances and arrangements concerning data-intensive digital platforms in recent years.

Concerns include issues related to the impact of increased commercialization, very sensitive and pervasive nature of the data these companies collect and use, and the potential consequences thereof, of children's rights to privacy and data protection, the responsibilities for companies, and the need for responsive law, regulation, and policy frameworks that take children's concerns seriously. Children with disabilities also likely face a significant impost in terms of the 'costs of connection,' and, if general critiques of disability and data are to be credited, specific and notable experiences of and subject to 'data colonialism' (Couldry & Mejias, 2019). Such issues are most likely to be heightened in relation to children with disabilities—and this is something on which we urgently need authoritative research and baseline data.

Amidst the reflex focus on risk and responsibility, there is also the need to better understand, acknowledge, and support the everyday, innovative use of digital technologies by children with disabilities. A key social imaginary of children with disabilities and technology is the great boon, if not salvation, it can confer—as, for instance, in the way that the advent of iPads have been acclaimed as a 'revolution' in the lives of children with disabilities (Alper, 2015), supporting learning and classroom participation, as well as providing enhanced access to information, entertainment, and communication. Digital inclusion is crucial especially when it comes to children with disabilities. This is because emerging digital technologies if conceived, designed, and implemented by and with people with disabilities can properly deliver the kind of quantum leap in accessibility often promised. Also, the new kinds of exclusion that can be associated with data and digital technologies—evident in the implementation of automation, machine learning, and AI, for instance—can be best foreclosed or addressed.

To understand the various sides of digital futures alluded to here, it would be helpful if we can learn more about how children with disabilities' view, secure, and finesse their privacy rights, ownership, and control of their information and data, in the process of forging their own paths to negotiating digital life and becoming and being citizens. Here we point to the important work undertaken by Amanda Third, Philippa Collin, Sonia Livingstone, and other children digital media and rights researchers in collaboration with UNICEF and NGOs that seeks to include children with disabilities and their voices, and put these at the centre of research and policy agenda (Livingstone & Third, 2017; Third, Bellerose, Oliveira, Lala, & Theakstone, 2017; Third & Collin, 2016).

Having sketched this larger backdrop and agenda, we offer a brief case study of privacy and data issues raised from a relatively common and recognizable scenario: the sharing of information on children with disabilities by their parents via social media platforms, so-called 'sharenting.' What this case study vividly indicates is a fundamental axis of power relations that shapes privacy and data for this ground. Namely, children with disability are rarely considered the owners of their private information. From their parents, to charity organisations to medical discourse writ large, the private lives of children with disability are considered public domain.

3. Scenes from "Sharenting" on Social Media

Just prior to Christmas 2015, the website *The Mighty*, at that time 'disability' branded and very widely promoted in this way, published an article entitled "Introducing: Meltdown Bingo" (the article is longer accessible, see Griffo, 2015). The squares in the bingo card in question included sensory and behavioural reactions a person with autism might experience while having a "meltdown." The suggestion was that parents could "play bingo" while their child has a meltdown brought on by the sensory overload of the festive season. The article described the way in which a mother referenced the Bingo card meme to draw attention to the challenging aspects of Christmas shopping and other activities for her family and in particular her eight-year-old son who has autism.

The mother and author of the piece also identified as being on the spectrum. However, the article was widely condemned by both disability and neurodiversity communities as being exploitative and damaging (Gibson, 2016) the dedicated #cripthemighty hashtag emerged in response, drawing on critical approaches to disability and autism (see Sinclair, 1993/2012). A critical approach to autism "[explores] power relationships that construct autism; [enables] narratives that challenge dominant negative medical autism discourses and [creates] theoretical and methodological approaches that are emancipatory and value the highly individual nature of autism and its nascent culture" (Woods, Milton, Arnold, & Graby, 2018, p. 975; see also Yergeau, 2018).

The Meltdown Bingo article is one example of a power relationship that constructs autism. It was interpreted as an example of both a large media organisation exploiting a disabled child for page views and a massive parental violation of privacy. Would the eight-year-old feel he was being made fun of? Would he be subject to bullying at school? Why would a disability branded website publish an article that contributed to damaging representations of disability? The representation took a psychic toll on adults with autism who described being ridiculed their whole lives. As a result, *The Mighty* became embroiled in an online war with activists that was picked up by the mainstream media. Many adult bloggers with autism were consequently excommunicated from *The Mighty* vast online community, others left in protest, and the site underwent a complete rebranding.

The Mighty now describes itself as a "digital health platform." This rebranding from a disability focused site to one concerned with health is not a subtle change, it was a recognition that the organisation had never moved beyond a biomedical focus in the first place. Perhaps this was because it foregrounds the perspective of parents of children with disability over the voices of people with disabilities (see Logsdon-Breakstone, 2015).

Drawing on the theory of communication privacy management, we can see these various actors as engaged in a negotiation of privacy limits generating considerable boundary turbulence. Since this controversy, the privacy turbulence between disabled adults and so-called special needs parents has intensified across other online practices from sharenting to microcelebrity, family influencers, and calibrated amateurism (for a discussion of the practices see Abidin, 2017, 2018). Sharenting and communities of practice are of particular concern and our focus in this article.

Sharenting, a portmanteau of the words parent and sharing, refers to online practices of parents who broadcast details and/or images of their children's lives online, usually on social media. While sharenting is often criticised, some positive aspects are recognized. These often focus on the formation of communities of interest whereby parents form communities around particular experiences and embark on a process of learning together. Parents of children with disability can become deeply embedded in these communities.

More recently, there has been the phenomenon of so-called family influencers who post videos of their children with autism experiencing extreme emotional states (popularly called "meltdowns"). According to these families these videos amass the most views and offer a potential to monetise content (Borgos-Rodriguez, Ringland, & Piper, 2019). However, these families emphasize that providing support and community is their real motivation. Making aspects of their lives public for the benefit of others is in stark contrast to offline studies where parents would only disclose their child's autism diagnosis if by doing so their child would benefit (Hays & Butauski, 2018). Indeed, some studies show that parents of children with disability report less social stigma in online communities (Ammari, Morris, & Schoenebeck, 2014).

According to Tama Leaver (in press) parents balance three points of privacy practices with and for their children in digital contexts: privacy stewardship, boundary turbulence, and intimate surveillance. In relation to instances such as the "sharenting" cases we discuss, an issue for disability lies in the ways biomedical and charity discourses of disability influence conventions surrounding this balancing and the creation of "privacy rules." The analysis is informed by a social, political, cultural, and rights-based approach to disability. This approach problematizes biomedical and charity discourses of disability. The image of the cute disabled child has long been leveraged by charity organisations trying to raise funds (Hevey, 1992; Longmore, 2005) or more recently as click bait (Young, 2012; Ellis, 2015). This image is achieving greater potency in user generated contexts and as mommy blogging moves through to microcelebrity and family influencers. Yet the parents themselves may have different motivations.

The theory of communication privacy management, advanced by Sandra Petronio posits that "people make choices about revealing or concealing based on criteria and conditions that they perceive as salient, and that individuals fundamentally believe they have a right to own or regulate their private information" (Petronio, 2002, p. 2). The decision to reveal also depends on how this information may affect other people. Petronio (2002) identifies five criteria of privacy management: ownership, control, privacy rules, shared ownership, and boundary turbulence. While Leaver's (in press) analysis foregrounds an assumption of shared ownership as optimal, children with disability do not always have this opportunity as parents often assume full not co-ownership of private information.

Parents engage in a process of communication privacy management when they share information about and/or images of their children online. The issue of sharenting on social media has received significant scholarly and media attention; however, there is none from a critical disability perspective of which we are aware. In academic discussions disability is almost always conflated with health and often functions as a narrative prosthesis (see Mitchell & Snyder, 2000) for the benefits of sharenting; whereby parents of children with disability can share their struggles online to gain support, or alternatively offer support for new parents. In effect, in this dominant view, parents assume the role as the active and important agents in the discussion, with children with disability serving as a widely accepted key site of social anxiety. The sum total of this arrangement is a reinforcement of pervasive social assumptions that "other" and stigmatize people with disability.

The oversharing of images and details of their children's lives that would have previously been considered private on social media is a common practice amongst parents. As the regulators of their children's privacy limits, these parents, not their children, are the ones deciding what to reveal or conceal. Academic analysis has largely focused on parental motivation rather than offering a clear definition of the practice, when it becomes problematic, and at a deeper level, what kinds of social relations are at stake in framing children with disabilities, their voices, data, and privacy (or lack thereof) in this way. Practical rather than ideological factors influencing decision making are usually the focus. For example, in a study focused on mothers, Kumar and Schoenebeck (2015) observe the development of a community of practice:

> Mothers use the Internet to seek information, advice, and support. Sharing information about one's children online provides social capital benefits. Women who participate in 'mommy blogging' enjoy validation and solidarity, develop a sense of community with others, and may experience greater wellbeing and increased feelings of connectedness. (p. 1304)

Despite this and other studies' focus on mothers, fathers also seek out communities of shared interest and collective learning. In a study of new parents' use of social media, Bartholomew, Schoppe-Sullivan, Glassman, Kamp Dush, and Sullivan (2012) found that while 98% of new mothers post images of their children for the purpose of building community on social media, 89% of fathers do likewise. Indeed, fathers are documenting and discussing their experiences of fatherhood online as part of a broader cultural shift and reconstruction of caring masculinities (Scheibling, 2020). When compared to other parents, parents of children with "special education needs" actually use the internet less in general yet report using a wider variety of devices and spend more time "seeking information on their child's health" (Zhang & Livingstone, 2019, p. 7).

Advice and support are primary motivations for sharenting amongst this group. Similarly, from a health perspective, the creation of peer-to-peer support via online communities is recognized as "complementing existing health services" and providing emotional and practical support to other people who may face similar issues (Eysenbach, Stendal, Petrič, Amann, & Rubinelli, 2017). Positive aspects of sharenting have been identified by scholars, especially in when it comes to analysis of the sharenting practices of parents of children with disability, as Kopecky, Szotkowski, Aznar-Díaz, and Romero-Rodríguez (2020) explain: "Sharenting can also support the cooperation of parents whose children suffer from varying degrees of physical or mental disability, allowing to share good practice (what parents have tried and what is proved), they support each other, consult, etc." (p. 1). The difficulty in this position is that it is underpinned by a biomedical approach to disability in which disability is a problem located in the individual body in need of fixing. This speaks to a broader conflict between the medical model and social models of disability that parents of children with disability must navigate. As Sonia Livingstone and Alicia Blum-Ross (2020) reflect:

> Many parents we interviewed were attracted to the social model of disability for offering a language that supported their child as not being *less than*, along with its critical lens on "mainstream" society's inability to provide the support they and their child needed. At the same time, they drew on the "medical model" because this is the language typically employed by support services, and parents were often preoccupied with juggling appointments with medical or learning specialists in ways designed to manage or mitigate the effects of their child's disability. (p. 121)

Another compounding issue in many online communities in which sharenting is prevalent is that misinformation can be rife—for example some private Facebook groups were found to be advocating the use of bleach enemas as a cure for autism (Zadrozny, 2019). This is an extreme and life-threatening example that came to light due to the efforts of two mothers of children with disability who joined these groups and reported their activities.

In this way, parents of children with disability can likewise act as powerful allies. Returning to Livingstone and Blum-Ross' (2020) study, the use of online communication by parents of children with disability is "popular [though] not without its problems." There is a diversity of experience, some parents being unable to find community in an ocean of information and competing agendas while others report experiencing intense unwanted attention (Livingstone and Blum-Ross, 2020). For example, they profile the activities of one mother who changed her approach to blogging when one of her posts about parenting a child with autism went viral. Having approached the blog as a way to blow off steam, as she would in a social setting, when the post reached a large audience it suddenly became a privacy violation of her child's experience that she may have to answer to one day. Although blogging about her own frustrations, this mother was also representing her daughter's life and struggles. The experience raised ethical considerations about who has the right to speak and potentially being held to account by her daughter at some point in the future for speaking of her behalf (Livingstone & Blum-Ross, 2020).

This is a recurring concern for critics of the sharenting practices of parents of children with disability:

> Imagine a child who has behavior problems, learning disabilities or chronic illness. Mom or Dad understandably want to discuss these struggles and reach out for support. But those posts live on the Internet, with potential to be discovered by college admissions officers and future employers, friends and romantic prospects. A child's life story is written for him before he has a chance to tell it himself. (Kamenetz, 2019)

Scholars and influencers identify some privacy conventions that have been established over time such as not identifying the child by name and taking photos from behind, never showing the child's face. Two important privacy conventions observed by influencer Anna Whitehouse are "ensuring no bathtime or swimming suit or naked images are used" and considering how your child would feel reading the post in 10 years' time (Whitehouse, 2018). Parents of children with disability seeking advice and community online have been accused of flouting these conventions by high profile disability activists who highlight the dangers of sharing medical or personal details (Counsel, 2019). Kumar and Schoenebeck observe that parents take on a "privacy stewardship" for their children in which they decide and enforce what is appropriate to share about their children (Kumar & Schoenebeck, 2015). However, these parents, influenced by a medical approach to disability can make bad decisions. In addition, for some children with disability this stewardship may never end. The privacy of disabled children is a concern for disabled adult bloggers who attempt to intervene by suggesting privacy conventions such as writing anonymously, not sharing details about their child's difficult moments and offering tips to other parents in private (see Sequenzia, 2016).

Clearly, a minimal step required is that discussions of and practices of sharenting should move beyond a consideration of parent's motivations to establish boundaries around this mode of communication (Brosch, 2018, p. 78). Bosch points out, further, that a definition of sharenting must also consider the potential for a mass audience, the possibility of identifying the child and the ways these come together as a privacy violation. She offers a framework for establishing the "true level of sharenting and classifying parents" (Brosch, 2018, p. 80) that takes into account "the amount, frequency, content of posted information and the audience" (Brosch, 2018, p. 79). In Livingstone and Blum-Ross's (2020) example, the attention of a mass audience prompted that mother to radically rethink her privacy stewardship to the extent that she helped her daughter construct her own blog, to speak for herself. Drawing on Cynthia Lewiecki-Wilson (2003), Livingstone and Blum-Ross (2020) describe this as a process of co-constructing language. However, returning to *The Mighty* controversy with which we began this discussion, that mother too had claimed to co-construct the article with her son, yet it could not be described as giving him voice. The key issue for disability activists was the way disability was leveraged to attract a larger audience. In order to provide peer support for parents of children with disabilities, *The Mighty* reinforced "well-worn negative tropes, clichés, and stereotypes about disability" (Bad Cripple, 2016).

In a parallel to critiques of sharenting in online communities, adult disability activists criticise the focus on memoirs published by parents (Jack, 2014; Sousa, 2011). For disability activist Emily Ladau (2016) these and other media directed towards supporting parents of children with disability while usually well intentioned can become problematic if parents do not "relinquish their positions of authority and move to the role of advocate-allies, advocating alongside, instead of on behalf of, disabled people" (Ladau, 2016) as their children age. Admittedly a fraught relationship, there is evidence too that strong relationships with parents of children with disability can be an important and strategic alliance for disability activists (Carey, Block, & Scotch, 2020).

4. Reflections on Data, Privacy, and Digital Futures for Children with Disabilities

In this article, we have sought to identify and lay out some of the issues in approaching and framing concerns of data and privacy for children in disabilities. One stumbling block to advancing research and understanding in this area is that critical disability approaches and concepts still need to be better understood in the fields of media and communication. However, there is clearly an opportunity, as we have endeavoured to suggest, to think critically and creatively about disability and privacy in the lives of children as they rely upon digital technologies.

To convey a sense of the issues and stakes at play, we focussed on one leading example: that of sharenting in social media. It is a useful and illustrative example because it lays bare some of the practices, power relations, and deeply held views that frame privacy, personal information, and data of children with disabilities. As we note, the boundary turbulence occurring throughout these examples is not so much between the parent and child but between two discrete communities: adults with disabilities and special needs parents. These groups have much in common but digress on key issues related to the online privacy of children with disabilities. Tama Leaver (in press) observes a continuum of approaches parents take to the sharing of their children's images online. At one end of the continuum, parents trade privacy for commercial success while at the other parents take a more privacy-centred approach. In the tensions that constitute this field, children with disabilities do not get much of a "look in," when it comes to articulating, in their own ways, via their own social and digital practices, what they think and feel about privacy.

This is all the more a pity, given it is a zone where good intentions concerning children with disabilities abound. Accordingly, if we can disentangle and constructively address the issues involved, this can be a productive point for understanding the fundamental underpinnings and values, as we tackle the issues raised by the infrastructures, technology companies, and providers that shape much of the environment in which social media communities, interaction, moderation, norms, and rules are constituted and contested, and build diverse coalitions and alliances of stakeholders around these. In addition to these overt privacy violations from parents, children with disability are also subject to more intense regimes of digital surveillance and the subsequent privacy issues that arise from having to use certain types of devices, wearables or even the many issues concerning surveillance, privacy, and data in relation to voice interfaces via Google, Facebook, or Amazon speakers. So, the agenda is wide and deep indeed.

To close on a positive note, there is good reasons to suggest that children with disabilities' evolving digital use practices themselves represents an opportunity for inclusion in conceptualization and debates concerning privacy—especially in relation to imagining and enacting good data frameworks and practices (Cranmer, 2020). This is an important area for future research, bringing together scattered work that does exist. Crucially, in research as well as policy and practice, the hallmark of genuine conceptual and social advance will be efforts that feature and are driven by children themselves reimagining good data futures for privacy-respecting disabled childhoods.

Acknowledgments

Our thanks to Rosemary Curtis for her proofreading this article.

Conflict of Interests

The authors declare no conflict of interests.

References

Abidin, C. (2017). #Familygoals: Family influencers, calibrated amateurism, and justifying young digital labor. *Social Media + Society*, *3*(2). https://doi.org/10.1177/2056305117707191

Abidin, C. (2018). *Internet celebrity: Understanding fame online*. Bingley: Emerald.

Ajodhia-Andrew, A. (2016). *Voices and visions from ethnoculturally diverse young people with disabilities*. Rotterdam: Sense.

Alper, M. (2014). *Digital youth with disabilities*. Cambridge, MA: MIT Press.

Alper, M. (2015). Augmentative, alternative, and assistive: Reimagining the history of mobile computing and disability. *IEEE Annals of the History of Computing*, *37*(1), 93–96. https://doi.org/10.1109/MAHC.2015.3

Alper, M. (2017). *Giving voice: Mobile communication, disability, and inequality*. Cambridge, MA: MIT Press.

Alper, M., & Goggin, G. (2017). Digital technology and rights in the lives of children with disabilities. *New Media & Society*, *19*(5), 726–740.

Ammari, T., Morris, M. R., & Schoenebeck, S. Y. (2014). Accessing social support and overcoming judgment on Social Media among parents of children with special needs. In E. Adar & P. Resnick (Eds.), *Proceedings of the Eighth International AAAI Conference on Weblogs and Social Media* (pp. 1–10). Palo Alto, CA: Association for the Advancement of Artificial Intelligence. Retrieved from https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/ammari_ICWSM2014.pdf

Bad Cripple. (2016). Cripping the mighty. *Bad Cripple*. Retrieved from http://badcripple.blogspot.com.au/2016/01/cripping-mighty.html

Bartholomew, M. K., Schoppe-Sullivan, S. J., Glassman, M., Kamp Dush, C. M., & Sullivan, J. M. (2012). New parents' Facebook use at the transition to parenthood. *Family Relations*, *61*(3), 455–469. https://doi.org/10.1111/j.1741-3729.2012.00708.x

Beckett, A. E., & Campbell, T. (2015). The social model of disability as an oppositional device. *Disability & Society*, *30*(2), 270–283. https://doi.org/10.1080/09687599.2014.999912

Benjamin-Thomas, T. E., Laliberte Rudman, D., Gunaseelan, J., Abraham, V. J., Cameron, D., McGrath, C., & Vinoth Kumar, S. P. (2019). A participatory filmmaking process with children with disabilities in rural India: Working towards inclusive research. *Methodological Innovations*, *12*(3). https://doi.org/10.1177/2059799119890795

Borgos-Rodriguez, K., Ringland, K. E., & Piper, A. M. (2019). MyAutsomeFamilyLife: Analyzing parents of children with developmental disabilities on YouTube. *Proceedings of the ACM on Human-Computer Interaction*, *3*, 1–26. https://doi.org/10.1145/3371885

Brosch, A. (2018). Sharenting: Why do parents violate their children's privacy? *The New Educational Review*, *54*(4), 75–85. https://doi.org/10.15804/tner.2018.54.4.06

Campbell, F. K. (2009). *Contours of ableism: The production of disability and abledness*. New York: Palgrave Macmillan.

Carey, A. C., Block, P., & Scotch, R. K. (2020). *Allies and obstacles: Disability activism and parents of children with disabilities*. Philadelphia, PA: Temple University Press.

Convention on the Rights of Persons with Disabilities, 2006.

Convention on the Rights of the Child, 1989.

Couldry, N. (2010). *Why voice matters? Culture and politics after neoliberalism*. Los Angeles, CA: Sage.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford, CA: Stanford University Press.

Counsel, J. (2019). What is sharenting? *My Aspie World*. Retrieved from https://myaspieworld.home.blog/sharenting

Cranmer, S. (2020). Disabled children's evolving digital use practices to support formal learning: A missed opportunity for inclusion. *British Journal of Educational Technology*, *51*(2), 315–330. https://doi.org/10.1111/bjet.12827

Ellcessor, E., & Kirkpatrick, B. (Eds.). (2017). *Disability media studies*. New York, NY: New York University Press.

Ellis, K. (2015). *Disability and popular culture: Focusing passion, creating community and expressing defiance*. Surrey: Ashgate.

Ellis, K., Goggin, G., Haller, B., & Curtis, R. (Eds.). (2020). *Routledge companion to disability and media*. New York, NY: Routledge.

Ellis, K., Goggin, G., & Kent, M. (in press). Disability, children, and the invention of digital media. In L. Green et al. (Eds.), *The Routledge companion of children and digital media*. New York, NY: Routledge.

Eysenbach, G., Stendal, K., Petrič, G., Amann, J., & Rubinelli, S. (2017). Views of community managers on knowledge co-creation in online communities for people with disabilities: Qualitative study. *Journal of Medical Internet Research*, *19*(10). https://doi.org/10.2196/jmir.7406

Foley, K. R., Blackmore, A. M., Girdler, S., O'Donnell, M., Glauert, R., Llewellyn, G., & Leonard, H. (2012). To feel belonged: The voices of children and youth with disabilities on the meaning of wellbeing. *Child Indicators Research*, *5*(2), 375–319. https://doi.org/10.1007/s12187-011-9134-2

Garland-Thomson, R. (2017). Eugenic world building and disability: The strange world of Kazuo Ishiguro's *Never Let Me Go*. *Journal of Medical Humanities*, *38*(2), 133–145. https://doi.org/10.1007/s10912-015-9368-y

Gibson, C. (2016, January 5). A disability-focused website ran a 'funny' post on autism: Anger ensued. *The Washington Post*. Retrieved from https://bit.ly/3cuHFpw

Goggin, G. (2009). Disability and the ethics of listening. *Continuum*, *23*(4), 489–502. https://doi.org/10.1080/10304310903012636

Goodley, D., Lawthom, R., Liddiard, K., & Runswick-Cole, K. (2019). Provocations for critical disability studies. *Disability & Society*, *34*(6), 972–997. https://doi.org/10.1080/09687599.2019.1566889

Griffo, M. (2015, December 22). Editor's note: Why we removed a story. *The Mighty*. https://themighty.com/2015/12/editors-note-why-we-removed-a-story

Hadley, B. (2014). *Disability, public space performance and spectatorship: Unconscious performers*. Houndsmill: Palgrave Macmillan.

Harris, J. E. (2020). The privacy problem in disability antidiscrimination law. In A. Silvers, C. Shachar, I. G. Cohen, & M. A. Stein (Eds.), *Disability, health, law, and bioethics* (pp. 159–170). Cambridge: Cambridge University Press.

Hays, A., & Butauski, M. (2018). Privacy, disability, and family: Exploring the privacy management behaviors of parents with a child with autism. *Western Journal of Communication*, *82*(3), 376–391. https://doi.org/10.1080/10570314.2017.1398834

Hevey, D. (1992). *The creatures time forgot: Photography and disability imagery*. London: Routledge.

Iarskaia-Smirnova, E. (2020). "It's no longer taboo, is it?" Stories of intimate citizenship of people with disabilities in today's Russian public sphere. *Sexuality & Culture*, *24*(2), 428–446. https://doi.org/10.1007/s12119-019-09699-z

Jack, J. (2014). *Autism and gender: From refrigerator mothers to computer geeks*. Champaign, IL: University of Illinois Press.

Jordan, A., & Prendella, K. (2019). The invisible children of media research. *Journal of Children and Media*, *13*(2), 235–240.

Kamenetz, A. (2019, June 5). The problem with 'sharenting.' *The New York Times*. Retrieved from https://www.nytimes.com/2019/06/05/opinion/children-internet-privacy.html

Kopecky, K., Szotkowski, R., Aznar-Díaz, I., & Romero-Rodríguez, J.-M. (2020). The phenomenon of sharenting and its risks in the online environment: Experiences from Czech Republic and Spain. *Children and Youth Services Review*, *110*. https://doi.org/10.1016/j.childyouth.2020.104812

Kumar, P., & Schoenebeck, S. (2015). The modern day baby book: Enacting good mothering and stewarding privacy on Facebook. In D. Cosley & A. Forte (Eds.), *CSCW '15: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 1302–1312). New York, NY: ACM. https://doi.org/10.1145/2675133.2675149

Ladau, E. (2016, January 13). The mighty question: Who should speak for the disability community? *Words I Wheel By*. Retrieved from https://wordsiwheelby.com/2016/01/the-mighty-question

Lansdown, G. (2014). Children with disabilities. In M. Sabatello & M. Schulze (Eds.), *Human rights and disability advocacy* (pp. 97–112). Philadelphia, PA: University of Pennsylvania Press.

Lazar, J., & Stein, M. A. (Eds.). (2017). *Disability, human rights, and information technology*. Philadelphia, PA: University of Pennsylvania Press.

Leaver, T. (in press). Balancing privacy: Sharenting, intimate surveillance and the right to be forgotten. In L. Green, D. Holloway, K. Stevenson, T. Leaver, & L. Haddon (Eds.), *The Routledge companion to digital media and children*. London: Routledge.

Lewiecki-Wilson, C. (2003). Rethinking rhetoric through mental disabilities. *Rhetoric Review*, *22*(2), 156–167. Retrieved from https://www.jstor.org/stable/3093036

Liddiard, K., Runswick-Cole, K., Goodley, D., Whitney, S., Vogelmann, E., & Watts, L. (2019). "I was excited by the idea of a project that focuses on those unasked questions": Co-producing disability research with disabled young people. *Children & Society*, *33*(2), 154–167.

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. New York, NY: Oxford University Press.

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, *19*(5), 657–670.

Logsdon-Breakstone, S. (2015). Run down of #CrippingTheMighty. *Cracked Mirror in Shalott*. Retrieved from https://crackedmirrorinshalott.wordpress.com/2015/12/23/run-down-of-crippingthemighty

Longmore, P. K. (2005). The cultural framing of disability: Telethons as a case study. *PMLA*, *120*(2), 502–508. Retrieved from https://www.jstor.org/stable/25486174

Maia, R. (2014). *Recognition and the media*. Houndsmill: Palgrave Macmillan.

McRae, L., Ellis, K., Kent, M., & Locke, K. (2020). Privacy and the ethics of disability research: Changing perceptions of privacy and smartphone use. In J. Hunsinger, M. Allen, & L. Klastrup (Eds), *Second international handbook of internet research* (pp. 413–429). Dordrecht: Springer. https://doi.org/10.1007/978-94-024-1555-1_66

Mitchell, D., & Snyder, S. (2000). *Narrative prosthesis: Disability and the dependencies of discourse*. Ann Arbor, MI: University of Michigan Press.

Montague, M. (1993). *Private lives? An initial investigation of privacy and disability issues: A discussion paper*. Melbourne: Office of the Public Advocate, Privacy Commissioner, Human Rights Australia.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–158. Retrieved from https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4450&context=wlr

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Oliver, M. (2013). The social model of disability: Thirty years on. *Disability & Society*, *28*(7), 1–3).

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: SUNY Press.

Price, M. (2011). *Mad at school: Rhetorics of mental disability and academic life*. Ann Arbor, MI: University of Michigan Press.

Priestley, M., & Shah, S. (2011). *Disability and social change: Private lives and public policies*. Bristol: Policy Press.

Roulstone, A. (2016). *Disability and technology: International and interdisciplinary perspectives*. Basingstoke: Palgrave.

Runswick-Cole, K., Curran, T., & Liddiard, K. (Eds.). (2018). *Palgrave handbook of disabled childhood studies*. London: Palgrave Macmillan.

Scheibling, C. (2020). "Real heroes care": How dad bloggers are reconstructing fatherhood and masculinities. *Men and Masculinities*, *23*(1), 3–19. https://doi.org/10.1177/1097184X18816506

Schulze, M. (2010). *Understanding the UN Convention on the Rights of Persons with Disabilities*. New York, NY: Handicap International. Retrieved from http://www.handicap-international.fr/fileadmin/documents/publications/HICRPDManual.pdf

Schweik, S. (2009). *The ugly laws: Disability in public*. New York, NY: New York University Press.

Sequenzia, A. (2016). Privacy, and parental behaviour. *Ollibean*. Retrieved from https://ollibean.com/privacy-and-parental-behavior

Shakespeare, T. (2018). *Disability: The basic*. London and New York, NY: Routledge.

Sinclair, J. (2012). Don't mourn for us. *Autonomy, the Critical Journal of Interdisciplinary Autism Studies*, *1*(1). (Originally work published 1993). Retrieved from http://www.larry-arnold.net/Autonomy/index.php/autonomy/article/view/AR1

Sousa, A. C. (2011). From refrigerator mothers to warrior-heroes: The cultural identity transformation of mothers raising children with intellectual disabilities. *Symbolic Interaction*, *34*(2), 220–243. https://doi.org/10.1525/si.2011.34.2.220

Third, A., Bellerose, D., Oliveira, J. D., Lala, G., & Theakstone, G. (2017). *Young and online: Children's perspectives on life in the digital age*. (The state of the world's children 2017 companion report). Sydney: Western Sydney University. https://doi.org/10.4225/35/5a1b885f6d4db

Third, A., & Collin, P. (2016). Rethinking (children's and young people's) citizenship through dialogues on digital practice. In A. McCosker, S. Vivienne, & A. Johns (Eds.), *Negotiating digital citizenship: Control, contest, and culture* (pp. 41–59). London: Rowman & Littlefield International.

Thompson, J. B. (2011). Shifting boundaries of public and private life. *Theory, Culture, & Society*, *28*(4), 49–70.

Tremain, S. (Ed.). (2015). *Foucault and the government of disability*. Ann Arbor, MI: University of Michigan Press.

Twomey, R. F. (2010). *Employment law: Going beyond compliance to engagement and empowerment*. Boston, MA: McGraw-Hill Irwin.

Whitburn, B., & Plows, V. (Eds.). (2017). *Inclusive education: Making sense of everyday practice*. Rotterdam: Sense.

Whitehouse, A. (2018, April 27). Private: No access. *Mother Pukka*. Retrieved from https://www.motherpukka.co.uk/private-no-access

Woods, R., Milton, D., Arnold, L., & Graby, S. (2018). Redefining critical autism studies: A more inclusive interpretation. *Disability & Society*, *33*(6), 974–979.

Yergeau, M. (2018). *Authoring autism: On rhetoric and neurological queerness*. Durham, NC: Duke University Press.

Young, S. (2012). We're not here for your inspiration. *Ramp Up*. Retrieved from www.abc.net.au/rampup/articles/2012/07/02/3537035.htm

Zadrozny, B. (2019, May 21). Parents are poisoning their children with bleach to 'cure' autism: These moms are trying to stop it. *NBC*. Retrieved from https://www.nbcnews.com/tech/internet/moms-go-undercover-fight-fake-autism-cures-private-facebook-groups-n1007871

Zhang, D., & Livingstone, S. (2019). *Inequalities in how parents support their children's development with digital technologies: Parenting for a digital future* (Survey Report No. 4). London: London School of Economies, Department of Media and Communications. Retrieved from http://www.lse.ac.uk/media-and-communications/assets/documents/research/preparing-for-a-digital-future/P4DF-Report-4.pdf

About the Authors

Gerard Goggin is Wee Kim Wee Professor of Communication Studies at Nanyang Technological University, Singapore. He is also Professor of Media and Communications, University of Sydney. His books on disability, media, technology, and culture include the co-authored *Digital Disability* (2003), *Disability and the Media* (2015), and the co-edited *The Routledge Companion to Disability and Media* (2020). Gerard is also widely published on mobile media and communication, with his most recent book being *Apps: From Mobile Phones to Digital Lives* (2021).

Katie Ellis (PhD) is the Director of the Centre for Culture and Technology at Curtin University, Australia, and an internationally recognised expert on disability and digital access. She is the Author or Editor of 17 books including most recently *Disability and Digital Television Cultures* and, with Gerard Goggin, Beth Haller, and Rosemary Curtis, *The Routledge Companion to Disability and Media*.

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 4, Pages 229–238
DOI: 10.17645/mac.v8i4.3261

Article

Designing Technologies with and for Youth: Traps of Privacy by Design

Bieke Zaman

Mintlab, Institute for Media Studies, KU Leuven, 3300 Leuven, Belgium; E-Mail: bieke.zaman@kuleuven.be

Submitted: 15 May 2020 | Accepted: 10 August 2020 | Published: 10 November 2020

Abstract

Media and communication scholars studying young people's privacy often involve them in research in order to better understand their interactions with digital technologies. Yet there is a lack of research on how, when, and why it makes sense to involve young people in the design phase of new technologies and how data protection safeguards can be taken proactively by design. By engaging with the body of literature at the intersection of media and communication studies, participatory design, and child–computer interaction research, this article discusses how youth-centred design efforts risk falling into three traps of privacy by design, relating to: 1) the different degrees of decision power within and between child-centred design guidelines and participatory design with young people; 2) the involvement of young people in design as citizens versus consumers; and 3) the conditions under which their participation in design is empowerment rather than mere decoration. The contribution of this article is a critical, sociotechnical reflection on the challenges and opportunities of involving young people in privacy by design decision-making. The article concludes by outlining an agenda for participatory design within an encompassing empowerment and digital citizenship framework that invites young people to reflect on who they want to be in a data-driven society.

Keywords

digital citizenship; empowerment; participatory design; personal data; privacy; privacy by design; youth

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

Media and communication scholars are consulting young people during research in order to better understand their unique notions of privacy. Little is known, however, about the research efforts that feed into the design of new technologies and the role that young people (can/should) take in these efforts. This is a missed opportunity, as research insights should not only have societal value for policy-making, education, and parenting but also inform the design of new digital technologies (Donoso, Verdoodt, Van Mechelen, & Jasmontaite, 2016; Mainsah & Morrison, 2012). Research insights can form the basis for decisions on how to implement technical safeguards of data protection and adapt digital technologies to young people's needs, competencies, and expectations. Young people have the right to be heard in all matters affecting them, including with respect to digital technologies, not only as consumers and data providers but also as active co-designers. This gives them the opportunity to question, negotiate, and gain a better understanding of privacy and data protection issues (Dowthwaite et al., 2020), which in turn creates a pathway to digital skill development for empowerment (D'Ignazio, 2017; Iversen, Smith, & Dindler, 2018). The right of minors to be heard in all matters affecting them is a central premise of Article 12 of the United Nations Convention on the Right of the Child (UNCRC; United Nations, 1989). In UNICEF's comments on this provision, it is explained that this can be achieved either via direct consultation of young people or through a representative or an appropriate body (Viviers, 2014).

When designing digital technologies, companies generally consider the regulatory framework to be the maximum level of data protection, whereas the needs and expectations of Internet users go beyond these legal provisions (Culnan & Williams, 2009; imec, 2019). Data protection regulation tells us what not to do with data, but gives little guidance on how to protect young people's interest and respect their rights by design (Lievens & Verdoodt, 2018). Clearly, there are many social and ethical challenges at stake that research on and with young people can reveal. An example is the rich research insights that show how teenagers enjoy online public exposure and social prestige within what they perceive and co-construct as meaningful, intimate peer networks, outside parental control and beyond technical age limits (Balleys & Coll, 2017; De Leyn, De Wolf, Abeele, & De Marez, 2019; Lievens & Verdoodt, 2018; Marwick & boyd, 2014). A decade ago, Culnan and Williams (2009, p. 674) called upon organisations to not only pursue legal compliance but also to take up a moral responsibility to protect consumer data and avoid causing harm. They argued for a culture of privacy with managerial moral responsibility and accountability for the organization's privacy behaviours and the implications these may have for people personally.

Waiting for digital technologies to be launched before considering measures that would better protect young consumers' best interests, gives very little incentive to companies to implement change. The incentives for the end-user to take privacy matters into their own hands are also anything but attractive. Even though young people like having control of their personal data (Dowthwaite et al., 2020), they avoid the hassle needed to achieve this (Compañó & Lusoli, 2010). People of all ages express paradoxical perceptions of responsibility for data protection, attributing responsibility to companies or to themselves (Fiesler & Hallinan, 2018), even if they believe they do not have the necessary skills to do so (Compañó & Lusoli, 2010). As it is difficult to make changes once technologies are on the market, both for companies and for users, more research is needed on how best to serve the interests of young people from the very beginning of the conceptualization and design of digital technologies. This would make it possible to take proactive rather than reactive measures.

Although involving young people in the design of new technologies is a key value in the field of child–computer interaction research (Kawas et al., 2020), little attention has been given on how to engage them in decision-making with respect to privacy and data protection (Hourcade et al., 2017). Child–computer researchers have called for privacy issues to be addressed more explicitly by adopting a participatory and multidisciplinary perspective (Hourcade et al., 2018). Privacy researchers in both computer sciences and social sciences have arrived at a similar conclusion: Privacy is not simply a technical matter, it must be understood in terms of situated and collective, networked practices (Dourish & Anderson, 2006; Marwick & boyd, 2014). In order to (re)consider privacy in the context of today's technological affordances, as this article will further argue, insights from science and technology must be combined with media and communication studies in a participatory approach that accounts for the views and experiences of young people.

In response, this article provides a critical sociotechnical reflection on the potential of young people as co-designers of a youth-friendly, privacy-sensitive digital future. Based on the insights in the fields of participatory design, child–computer interaction research, and media and communication studies, three traps of privacy by design are identified. In what follows, this article discusses for each trap where and why the involvement of young people in design presents challenges and opportunities. The findings will show that young people's involvement in privacy by design efforts is as much about the improved and better design outcomes that can lead to a better quality of life in the long term, as it is about how young people can benefit from the process of participating in design.

2. Trap #1: Questioning Where the Decision Power Resides

Design decision-making is a matter of exercising power (Frauenberger, Good, Fitzpatrick, & Iversen, 2015). It provides an opportunity for the redistribution of power by including the typical "have-nots" in shaping their future (Arnstein, 2019, p. 24). Design decision power generally resides in adults who develop and design technologies for young people and who create policies and regulations for their use. There are regulations relating to design that pay particular attention to the protection of personal data for those under the age of 18. Examples include the European Union's General Data Protection Regulation (European Parliament, 2016), the Children's Online Privacy Protection Act in the United States (Lievens & Verdoodt, 2018), and child-centred design guidelines, such as the list of 16 'standards of age-appropriate design' of the UK's Information Commissioner's Office (ICO; Livingstone, 2019). Child-centred design guidelines are a good example of a knowledge dissemination format that can build a much-needed bridge between academia and practice (Donoso et al., 2016). It can also help to alleviate some of the difficulties implementing the data regulations into concrete design decisions that support young people's best interests (Dowthwaite et al., 2020; Lievens & Verdoodt, 2018). For instance, the ICO's list promotes the protection of personal data, compliant with the GDPR and UNCRC, and documents concrete child-centred design principles revolving around issues of 'data minimisation,' 'transparency,' 'default settings,' and 'parental controls' (ICO, 2019). Child-centred design guidelines such as the ICO's are not neutral design resources. Even though they were introduced as "technology-neutral design principles and practical privacy features" (ICO, 2019, p. 16), they do serve as normative expectations about young people's interactions with technology (Yu, Stoilova, & Livingstone, 2018). Each list of guidelines will always make certain aspects significant, while ignoring or giving less weight to other aspects and different values, for instance by emphasizing specific risks or opportunities. They implicitly or explicitly communicate what can be understood as acceptable and adequate media use. Even in the way design documentation seeks credibility, it is not neutral. Does it report on the consultation of experts (and what kind of experts) to justify the content? And to what extent were young people heard in this process? The answers to these questions reveal the extent to which these guidelines are an instrument in the hands of the typical haves or have-nots. Child-centred design guidelines are not fully prescriptive either. There will always be a dozen possible 'translations' in concrete design features, and hence this gives considerable room to exert influence. As long ago as 1985, computer ethics researcher James H. Moor compared writing a computer programme with building a house: "No matter how detailed the specifications may be, a builder must make numerous decisions about matters not specified in order to construct the house" (Moor, 1985, p. 7). Reaching the right practical level is a challenging undertaking. If the guidelines are too specific, they lose their applicability to a broad realm of services; too abstract, they risk becoming opaque and hard to interpret. This difficult balance brings both challenges and opportunities. On the one hand, there is always a risk of getting lost in translation, because the design guidelines do not say how they should be translated into concrete design features, how to assess and choose from the different alternatives, or how to ensure and evaluate whether the design choices are sufficiently youth-friendly and future proof to embrace all possible use(r)s and transformations. On the other hand, open-ended design guidelines also offer opportunities because they give flexibility for those involved in the design process to respond to cultural practices and context-specific demands (Nissenbaum, 2010). If open-endedness is built into the final design, then it also lowers the barriers for people to appropriate digital technology, as a co-designer during use.

In order to overcome the translation and implementation challenges mentioned above, previous research has argued for the participation of young people in design efforts. This would avoid overly adult-oriented interpretations and ensure that privacy by design choices are meaningful, attractive, and understandable to young people (Dowthwaite et al., 2020; Lievens & Verdoodt, 2018; Wauters, Donoso, & Lievens, 2014). Next to pragmatic considerations, the involvement of people in design can also be driven by a moral commitment to redistribute decision-making power. The latter approach has been amply described in the field of participatory design research. Its roots are situated in the political economy and worker's movement of the 1960s and 1970s in Scandinavian countries. It built on the premise that people who must live with the consequences of the introduction of technologies have the right to influence the changing conditions. Since its early years, the scope of participatory design research has been expanded by moving beyond the work context (Halskov & Hansen, 2015), and by diversifying collaboration, including research with young people as design stakeholders (see e.g., Druin, 1998; Markopoulos, Read, MacFarlane, & Hoysniemi, 2008). Notwithstanding more than 30 years of research on participatory design, there is a lack of a shared definition of what exactly it is. The field is characterized by a great diversity of design practices (Halskov & Hansen, 2015) that build on a number of common key features. One of those common characteristics being the use of participatory methods as a means to give people influence on design decisions (Halskov & Hansen, 2015). It provides an alternative model to the hierarchical expert (adult) versus (child) user power relations (Cumbo, Eriksson, & Iversen, 2019). Participatory design is more than the mere involvement of people in design; it is primarily a political commitment that "places the power of defining and reshaping use situations" in the hands of those affected by the technologies, "allowing them to transform their own lives" (Halskov & Hansen, 2015, pp. 89–90). In doing so, participatory design pursues change. In the narrowest sense, change refers to the exploration of design alternatives that could yield improved or better products. Beyond the product focus, there is also a concern about the benefits of participation in the process, for instance linked to learning opportunities. In the broadest sense, participatory design has become increasingly concerned with exploring the role of technologies in improving the quality of life (Halskov & Hansen, 2015).

Within the diversity of participatory design practices, we discern various levels of participatory power depending on who (e.g., which young person is recruited?) is participating; why (e.g., to create a better product or because young people have the right to be heard?); how (e.g., which role do young people take in the design process?); to what extent (e.g., how is decision power shared between young people and adults?); and with what gains (e.g., how do young people benefit from participation?). In addition, we can distinguish between approaches that only focus on people's agency in the design and production of new technologies, and participatory design that continues when the project funding ends and that is also concerned with people's agency during use and consumption. Traditionally, participatory design typically involved young people in one or more iterative design phases aiming at a better or improved end product or system. The participation then finished with the creation of a product or system, as a rather fixed result developed within the project time. This contrasts with participatory design processes that fully account for the sociotechnical processes that unfold over the long term; here participation is seen as an important condition of building an ongoing, dynamic infrastructure, which does not finish when the project ends. This long-term perspective unfolds the range of activities for co-shaping technological affordances, from design time to ongoing design practices during use and consumption (Bjögvinsson, Ehn, & Hillgren, 2012; Löwgren & Reimer, 2013). Media scholars have linked the latter practices under the umbrella of young people's 'rights by design,' which allow them, for instance, to check, rectify, erase, or edit personal data (Yu et al., 2018). Lievrouw (2006) theorizes this as design opportunities for creatively reconfiguring the technological artefacts and for remediating content and forms of interaction practices. Similar voices emanate from international organisations, including companies, as part of an initiative that sets out the principles for a safer and more empowering positive future, led by Tim Berners-Lee. It includes principles that explicitly call upon adaptation, appropriation, and redesign practices that are part of the design in use time. As part of their proposed 'Contract for the Web,' people are invited to be engaged as co-creators, actively shaping online content and systems and building strong online communities (Contract for the Web, 2019). Approaching people as co-creators is also relevant in the context of privacy by design, "because contexts shift and overlap over time, privacy is an ongoing, active practice" (Marwick & boyd, 2014, p. 1062). Young people are active agents in this process, as they co-construct and give active meanings to privacy norms and contexts, not only during the design time of new technologies (Dowthwaite et al., 2020) but also as part of the use time once the technologies have been implemented (De Leyn et al., 2019; Marwick & boyd, 2014; Steijn & Vedder, 2015).

In sum, with the identification of the first trap, we made explicit that there are differences both within and between child-centred design guidelines and participatory design efforts, and that these differences reveal where the design decision-making power resides. We discussed that although design guidelines can create youth-centred sensitivities that feed into design decision-making, they should not be understood as a prescriptive list telling us exactly *what* to design. Considering *how* we can design for and with young people, we pointed to the importance of embracing young people's rights by design, not only as part of their consumption and use of technologies, but also during the conceptualization and design of these technologies before their actual implementation.

3. Trap #2: Young People Are More Likely to Participate in Design as Consumers Than as Citizens

As part of the second trap, this article elucidates how the different manifestations of participatory design are likely to boil down to an involvement of young people as consumers instead of citizens. One way of seeking genuine participation is to engage young people as citizens. Such an approach is being advocated in a reinvigorated research strand on participatory design concerned with building dynamic infrastructures that enable long-term engagement in a project or with respect to a societal issue (Bjögvinsson et al., 2012) through the formation of publics, for instance by matchmaking citizens with local organisations and governments, and by fostering civic engagement and building capacities to connect to, set up, and sustain communities (Le Dantec & DiSalvo, 2013; Le Dantec & Fox, 2015; Mainsah & Morrison, 2012). However, if young people are only involved because they represent the target group of the envisioned product, then we are likely to reach out to them in their economic role instead of that as a citizen. Their economic position can point to their role as a future consumer, future producer co-shaping infrastructural elements, or as future data provider (van Dijck, 2009). The reasoning then goes that if young people, as experts of their own lives, are given a voice in the design of products they will eventually use, we are likely to increase future adoption and create more successful (read: more useful and economically viable/competitive) products.

If 'learning from youth' is the only reason young people are involved, then we must face its downsides. Simply inviting young people to deliver ideas and inform us how they perceive issues of privacy management, and then stopping their participation once we have 'taken' from them what we need for research is not an empowered form of participation (Zimmerman, 2000). In a commercial setting, co-creation creates a tension between people's voices enabled by the professional entities versus those who are exploited for their ideas or labour (Banks & Humphreys, 2008; van Dijck, 2009). While academic research goes through a rigorous process of ethical reviewing, commercial participatory design projects in industry do not (Hourcade et al., 2017). The involvement of young people in the design process may even create datafied users before technologies are on the market and under regulatory scrutiny. Nowadays, the spheres in which participatory design unfold no longer operate in isolation from each other. The neoliberal 21st century research and technology commercialization ecosystem pursues innovation through collaboration and co-creational interactions that group industry, university, government, and societal stakeholders to better align commercialization efforts with the needs of society (Markman, Siegel, & Wright, 2008; McAdam, Miller, & McAdam, 2018). It remains to be seen how and whether the latter evolution serves the interests of young people.

Unfortunately, many design projects in which young people participate are in fact nothing more than a 'crowdsourcing of ideas' (Read, Fitton, Sim, & Horton, 2016). This reminds us of the 'work as play' trap and the technology-discourses that circulated in the geek culture of the digital creative industries that built on the volunteerism and digital labour of early adopters, enthusiasts, and hobbyists who loved to tinker with media (van Dijck, 2009, p. 51). Furthermore, the commercial context is dominated by a technocratic view on innovation that trumps social innovation and that promotes what Morozov (2013, p. 6) refers to as 'technological solutionism': the "unhealthy preoccupation with sexy, monumental, and narrow-minded [computational] solutions—the kind of stuff that wows audiences at TED Conferences—to problems that are extremely complex, fluid, and contentious." Technology design would therefore benefit from a holistic understanding of the problem space, to which participatory design research can contribute, because "what many solutionists may presume to be 'problems' in need of solving are not problems at all" (Morozov, 2013, p. 6). Morozov warns against techno-utopian discourses that suggest that technologies will save the world, just as he warns against unintended consequences of technological solutionism. As far as research into privacy by design is concerned, there is a possible (intended or unintended) side effect, namely that the mere involvement of young people would make them responsible for finding solutions to privacy issues or even relieve institutional responsibility. This would fall into the same trap as many technical and legal discourses around privacy that have made the individual responsible for maintaining control over personal data, even when it is clear that users do not fully understand what they are giving permission to and that people suffer from consent fatigue (Royakkers, Timmer, Kool, & van Est, 2018). Simply striving to improve the accessibility and readability of privacy policies and terms and conditions is not enough, as it still passes the responsibility for making informed choices on to the end-users (Fiesler & Hallinan, 2018). The current networked privacy context makes the focus on the individual untenable (Marwick & boyd, 2014). Therefore, privacy by design must be holistically understood as the mutually constitutive interactions between and among the people who use technologies as well as the platforms, third parties, policymakers, educators, and regulators who are all embedded in particular data practices. We must also refrain from reducing privacy to a micro-level concern as if the 'problem' and 'solution' is only to be found in design properties. Economic, governance, and cultural issues play a role in shaping any privacy by design effort. A multi-stakeholder and multi-layered notion of privacy is thus needed to respond to the societal and technical complexity and messiness of today's data-driven society (Barassi, 2018; van Dijck, 2009). Just like techno-utopian discourses can cause blind spots, so too techno-dystopian discourses and media panics have side effects. The latter discourses may incite companies to take actions to protect young people against what adults see as risks, which is not always experienced as such by young people themselves (Lobel, Granic, Stone, & Engels, 2014). It may even prompt companies to stop offering their services to young people altogether, thereby thwarting their digital participation rights (Lievens & Verdoodt, 2018).

Applauding participatory design with young people to some extent mirrors how we have hailed the surge of young people using the digital space as part of the participatory culture (van Dijck, 2009). If we draw lessons from how the participatory culture has evolved, we learn that a transformation has taken place, whereby participatory media have transformed from small initiatives towards a mastodon ecosystem of media conglomerates. Similarly, for the first research-driven participatory design projects that operated on a small scale, it was easier to pursue safeguards for democratic participation, both with respect to processes and outcomes. In contrast, today, with digital platforms that place young people's media consumption practices in the hands of big tech giants (van Dijck, 2009), the question is whether and how participatory design must follow and be adjusted to this new complexity (Bannon, Bardzell, & Bødker, 2018). Just like the participatory culture promoted by Web 2.0 did not succeed in opening real possibilities for democratic empowerment (Barassi, 2017), so might we question whether today's participatory design efforts risk falling victim to corporate exploitation of user's digital production and to biases caused by fake and commodified forms of empathy with the end-user (Robertson & Allen, 2018). Moreover, with technologies increasingly controlling life for us, the design choices underlying them risk promoting technological paternalism whereby, at design time and through design, what is best is decided, with less control for the diverse user group to make it work for them in a meaningful way (Royakkers et al., 2018, p. 131). Floridi (2014, p. 190) similarly argues "that *ethics by design* may be mildly paternalistic, insofar as it privileges the facilitation of the *right* kind of choices, actions, process, or interactions on behalf of the agents involved." In response, Floridi calls for 'pro-ethical design,' which privileges facilitation of reflection instead of the search for the 'right' choices.

In sum, with the identification of a second trap, this article argued that young people are more likely to participate in design as consumers than as citizens, and pointed to problematic discourses and practices when the sole motivation to involve young people in design is pragmatic and functionalist driven. Continuing the line of thought developed earlier that design guidelines *can* never be fully prescriptive, this statement is now reconsidered by positing that design guidelines *must* never be prescriptive either, but for ethical reasons. Deciding upon the 'right' privacy options for and by design, includes the risk of taking rigid moral decisions on what is right or best. Even when driven by good intentions, designing for good can mean different things for different people. Especially as by 'othering' those for whom the product is designed, as people in need of help, we easily risk being paternalistic (Vandenberghe & Slegers, 2016). Participatory design, then, should instead be seen as an opportunity to negotiate design options for continued meaning-making and for reflection by diverse user groups, rather than a momentary act to arrive at a single and fixed solution.

4. Trap #3: Young People's Participation in Design is More Often an Act of Decoration Than of Empowerment

An analysis of the last decade of research on the design of technologies for and with young people has revealed that more research is needed to understand how participation in design is linked to empowerment (Kawas et al., 2020). The third and last trap aims to address this issue by discussing the differences between acts and outcomes of empowerment versus decoration. Genuine participation should imply giving a certain degree of decision-making power to young people and to be, therefore, more than a tokenistic assurance that they will hear and be heard—without any ability to influence or change (Arnstein, 2019; Hart, 2008). In design, this would enable young people to negotiate the issues that concern them, by creating and deciding upon design choices (Wagner, 2018; Zimmerman, 2000). This boils down to empowerment as 'inclusion' in decision-making processes (Floridi, 2014). Additionally, we can think of empowerment in the 'more opportunities' sense, that is empowerment as 'improvement' (Floridi, 2014). The latter is pursued if the involvement of young people as co-designers aims for both a higher quantity of available choices and a higher quality of opportunities. Empowerment-led forms of participatory design resemble action research. They both build on an agentic notion of non-academic people, including youths, acknowledging their right and capacity to actively participate in research on topics that matter to them. Moreover, both action research and participatory design share a similar moral commitment to explore alternatives and possibilities for change through the participation in and outcomes of the research (Frauenberger et al., 2015; Kemmis, McTaggart, & Nixon, 2014). The envisioned change is typically linked to social and educational values that the research participants can benefit from. Both in action research and participatory design, researchers use terms as 'empowerment,' 'gains,' 'benefits,' 'democracy,' and 'mutual/collaborative learning' to describe the goals of their participatory research endeavours (see e.g., Donoso et al., 2016; Frauenberger et al., 2015; Halskov & Hansen, 2015; Iversen et al., 2018; Kemmis et al., 2014; Kinnula et al., 2017; Schepers, Dreessen, & Zaman, 2018b). From the perspective of empowerment theory, the impact of change can be situated at the individual, community, and/or organisational levels (Zimmerman, 2000). Most empowerment efforts pursue individual benefits, for instance, linked to acquiring decision-making skills or critical awareness (Zimmerman, 2000). Although participatory design projects have also mainly been concerned with individual empowerment (Bjögvinsson et al., 2012), we are witnessing an increased interest in organizational and community concerns (Le Dantec & DiSalvo, 2013; Le Dantec & Fox, 2015; Mainsah & Morrison, 2012).

Empowerment theory not only accounts for individual, organizational, and community levels, and empowerment as inclusion versus empowerment as improvement, it also distinguishes between the 'empowering' processes and being 'empowered' as an outcome (Zimmerman, 2000). In the field of participatory design, both aspects have been addressed, with researchers investigating the empowering potential of the methods and procedures of participation in design as well as the positive change that is envisioned with it (see e.g., Halskov & Hansen, 2015; Iversen, Smith, & Dindler, 2017; Schepers, Dreessen, & Zaman, 2018a; Schepers et al., 2018b). Both processes and outcomes should not be understood as momentary acts, or as individual one-off events. From the very outset, the participatory design community was built on the principle of dialectical exchanges and mutual learning (Bratteteig, Bødker, Dittrich, Mogensen, & Simonsen, 2013; Halskov & Hansen, 2015). This implies a commitment to the involvement of people in design, as well as a commitment to give something back. In and through participatory design with young people, researchers and designers learn about young people's opinions, perceptions and experiences, and their situated actions. By opening up dialogue, adults learn about the particularities of youth culture in which privacy is perceived and negotiated. Young people, in turn, through their participation in research and design, acquire new competencies, such as the knowledge, skills, and attitudes to critically and constructively engage with technology, which Iversen et al. (2018) have called 'computational empowerment.' In line with empowerment theory, computational empowerment builds on a moral commitment to co-create positive change and identify strengths, which is more than just ameliorating negative aspects or identifying risks. As computational empowerment accounts for the educational aspects of engagement with technologies, as well as the economic and civic/political opportunities, this article argues, it is an important steppingstone towards digital citizenship. Building on a review of over 35 frameworks on youth and digital citizenship over the world, Cortesi, Hasse, Lombana, Kim, and Gasser (2020) have put forward a definition for what they term 'digital citizenship+ (plus),' that is, "the skills needed for youth to participate fully academically, socially, ethically, politically, and economically in our rapidly evolving digital world" (p. 28). Through co-design activities with young people, Cortesi et al. (2020) mapped 17 interconnected areas of life that they believe youth digital citizenship programmes should address, including amongst others artificial intelligence, civic and political engagement, computational thinking, data, and privacy and reputation. As it is an encompassing, balanced term, open for contextualized interpretations, it holds the potential to provide a valuable framework for future contributions in the realm of privacy by design theory and practice.

By identifying the third trap, this article aims to reverse the trend that young people's participation in design is more often an act of decoration than of empowerment. This would require reflection on both the processes and outcomes of the involvement of young people ("are these empowering processes resulting in young people being empowered?"), the flavour of being empowered (in a sense of both inclusion and improvement), as well as a consideration of both the challenges and opportunities for digital citizenship that reside and interact at an individual, organizational, and community level.

5. Conclusions

The rationale for this article followed from the observation that most media and communication studies dealing with youth and privacy have only been concerned with hearing young people's voices regarding their interaction with existing technologies. Yet, considering the timeline of a technology's trajectory, this article argued that we should not only study (the broad array of societal changes that may arise from) the adoption and use of digital technologies but also consider how design decisions are being made prior to their implementation (see also e.g., Bailey & Barley, 2020). This would give scholars opportunities to support young people's best interests proactively rather than reactively when privacy issues are flagged, e.g., by legislative bodies or through bad publicity (Culnan & Williams, 2009; Fiesler & Hallinan, 2018). This article aimed to address the gap in research on how, when, and why it makes sense to involve young people in design decision-making prior to the implementation of digital technologies. It did so by engaging with literature from existing schools of thought that speak to media and communication as well as to disciplines concerned with the (participatory) design, evaluation, and implementation of interactive computing systems. The contribution of this article revolves around the identification of three traps of privacy by design. The first trap pointed to different degrees of decision power in relation to the use of child-centred guidelines and participatory design research with young people. The second trap revealed the wide variety of approaches that all fit within the umbrella term of participatory design, but that differ in whether they involve young people as consumers or citizens. Finally, the third trap made clear how participatory design with young people can serve empowerment rather than being a decoration.

In conclusion, it is argued that participatory design situated within an encompassing empowerment and digital citizenship framework is a future-proof direction beneficial to young people. In today's increasingly complex and messy digital society, we must not blindly focus on the question of whether young people have comprehensive knowledge (see also Article 12 of the UNCRC) of the privacy issues at stake. We must also move beyond the discussion of whether young people can really implement change at the levels of commercial and institutional privacy, areas that they are not immediately concerned with (Steijn & Vedder, 2015), and that rather call for a reflection on data governance strategies on a macro level. In a world where humans are increasingly losing power and control to machines, and where even adults and the traditional institutes have a hard time following the rapid pace of technology, it is more beneficial to rethink our traditional notions of participatory design, as the entire 'human-centred design' logic seems to be at odds with current developments. Rather than seeking input through participative design with young people on what must be designed, and deciding upon the 'right' design choices, it is more fruitful to seek an answer to the question of what kind of society we want regarding our interaction with technology (Frauenberger, 2019), as well as how we can build in mechanisms for an ongoing reflection on this compelling question (Floridi, 2014), both during design in production time and during design in use and consumption. This approach would also help us to reflect on how privacy issues are interlinked with other public values, that is not only with the value of security—as amply covered in public debates—but also with public values that are given less attention, such as autonomy, human dignity, and control (Royakkers et al., 2018, p. 128). Future researchers and designers are therefore called upon to take the unique meaning-making processes and experiences of young people as a starting point, not only to improve or mitigate risky, harmful, and undesirable (privacy-related) design issues, but also to facilitate a contextualized reflection on who young people want to be in a data-driven society.

Acknowledgments

I am grateful to Selina Schepers, Marije Nouwen, Jessica Schoffelen, Luciana Monteiro Krebs, Katleen Gabriels, Bert Vandenberghe, Mariek Vanden Abeele, Ralf De Wolf, Timothy Kariotis and the anonymous reviewers for their inspiration.

Conflict of Interests

The authors declare no conflict of interests.

References

Arnstein, S. R. (2019). A ladder of citizen participation. *Journal of the American Planning Association*, *85*(1), 24–34. https://doi.org/10.1080/01944363.2018.1559388

Bailey, D. E., & Barley, S. R. (2020). Beyond design and use: How scholars should study intelligent technologies. *Information and Organization*, *30*(2), 100286. https://doi.org/10.1016/j.infoandorg.2019.100286

Balleys, C., & Coll, S. (2017). Being publicly intimate: Teenagers managing online privacy. *Media, Culture & Society*, *39*(6), 885–901. https://doi.org/10.1177/0163443716679033

Banks, J., & Humphreys, S. (2008). The labour of user co-creators: Emergent social network markets? *Convergence: The International Journal of Research into New Media Technologies*, *14*(4), 401–418. https://doi.org/10.1177/1354856508094660

Bannon, L., Bardzell, J., & Bødker, S. (2018). Reimagining participatory design. *Interactions*, *26*(1), 26–32. https://doi.org/10.1145/3292015

Barassi, V. (2017). BabyVeillance? Expecting parents, online surveillance and the cultural specificity of pregnancy apps. *Social Media + Society*, *3*(2), 1–10. https://doi.org/10.1177/2056305117707188

Barassi, V. (2018). The child as datafied citizen: Critical questions on data justice in family life. In G. Mascheroni, A. Jorge, & C. Ponte (Eds.), *Digital parenting: The challenges for families in the digital age* (pp. 169–177). Gothenburg: Nordicom. https://research.gold.ac.uk/23737

Bjögvinsson, E., Ehn, P., & Hillgren, P.-A. (2012). Design things and design thinking: Contemporary participatory design challenges. *Design Issues*, *28*(3), 101–116. https://doi.org/10.1162/DESI_a_00165

Bratteteig, T., Bødker, K., Dittrich, Y., Mogensen, P. H., & Simonsen, J. (2013). Methods: Organising principles and general guidelines for participatory design projects. In J. Simonsen & T. Robertson (Eds.), *Routledge international handbook of participatory design* (p. 117). Abingdon: Routledge. https://www.bookdepository.com/Routledge-International-Handbook-Participatory-Design-Jesper-Simonsen/9780415720212

Compañó, R., & Lusoli, W. (2010). The policy maker's anguish: Regulating personal data behavior between paradoxes and dilemmas. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of information security and privacy* (pp. 169–185). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-6967-5_9

Contract for the Web. (2019). *Contract for the Web*. Washington, DC: Contract for the Web. Retrieved from https://9nrane41lq4966uwmljcfggv-wpengine.netdna-ssl.com/wp-content/uploads/Contract-for-the-Web-3.pdf

Cortesi, S. C., Hasse, A., Lombana, A., Kim, S., & Gasser, U. (2020). *Youth and digital citizenship+ (plus): Understanding skills for a digital world* (Research Paper No. 2020–2). Cambridge, MA: Berkman Klein Center for Internet & Society. http://dx.doi.org/10.2139/ssrn.3557518

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673. https://doi.org/10.2307/20650322

Cumbo, B. J., Eriksson, E., & Iversen, O. S. (2019). The "least-adult" role in participatory design with children. In A. Lugmayr, M. Masek, M. Reynolds, & M. Brereton (Eds.), *Proceedings of the 31st Australian Conference on Human-Computer-Interaction* (pp. 73–84). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3369457.3369464

De Leyn, T., De Wolf, R., Abeele, M. V., & De Marez, L. (2019). Reframing current debates on young people's online privacy by taking into account the cultural construction of youth. In A. Gruzd, P. Mai, & P. Kumar (Eds.), *Proceedings of the 10th International Conference on Social Media and Society: SMSociety '19* (pp. 174–183). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3328529.3328558

D'Ignazio, C. (2017). Creative data literacy: Bridging the gap between the data-haves and data-have nots. *Information Design Journal*, *23*(1), 6–18. https://doi.org/10.1075/idj.23.1.03dig

Donoso, V., Verdoodt, V., Van Mechelen, M., & Jasmontaite, L. (2016). Faraway, so close: Why the digital industry needs scholars and the other way around. *Journal of Children and Media*, *10*(2), 200–207. https://doi.org/10.1080/17482798.2015.1131728

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, *21*(3), 319–342. https://doi.org/10.1207/s15327051hci2103_2

Dowthwaite, L., Creswick, H., Portillo, V., Zhao, J., Patel, M., Perez Vallejos, E., . . . Jirotka, M. (2020). "It's your private information. It's your life.": Young people's views of personal data use by online technologies. In E. Rubegni & A. Vasalou (Eds.), *Proceedings of the Interaction Design and Children Conference* (pp. 121–134). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3392063.3394410

Druin, A. (Ed.). (1998). *The design of children's technology*. San Francisco, CA: Morgan Kaufmann.

European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation. Brussels: European Parliament. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

Fiesler, C., & Hallinan, B. (2018). "We are the product": Public reactions to online data sharing and privacy controversies in the media. In R. Mandryk & M. Hancock (Eds.), *Proceedings of the 2018 CHI conference on Human Factors in Computing Systems: CHI '18* (pp. 1–13). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3173574.3173627

Floridi, L. (2014). *The 4th revolution: How the infosphere is reshaping human reality* (1st ed.). Oxford: Oxford University Press.

Frauenberger, C. (2019). Entanglement HCI the next wave? *ACM Transactions on Computer-Human Interaction*, *27*(1), 1–27. https://doi.org/10.1145/3364998

Frauenberger, C., Good, J., Fitzpatrick, G., & Iversen, O. S. (2015). In pursuit of rigour and accountability in participatory design. *International Journal of Human-Computer Studies*, *74*, 93–106. https://doi.org/10.1016/j.ijhcs.2014.09.004

Halskov, K., & Hansen, N. B. (2015). The diversity of participatory design research practice at PDC 2002–2012. *International Journal of Human-Computer Studies*, *74*, 81–92. https://doi.org/10.1016/j.ijhcs.2014.09.003

Hart, R. A. (2008). Stepping back from 'the ladder': Reflections on a model of participatory work with children. In A. Reid, B. B. Jensen, J. Nikel, & V. Simovska (Eds.), *Participation and learning* (pp. 19–31). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-6416-6_2

Hourcade, J. P., Zeising, A., Antle, A. N., Anthony, L., Fails, J. A., Iversen, O. S., . . . Walsh, G. (2018). Child-computer interaction, ubiquitous technologies, and big data. *Interactions*, *25*(6), 78–81. https://doi.org/10.1145/3274572

Hourcade, J. P., Zeising, A., Iversen, O. S., Pares, N., Eisenberg, M., Quintana, C., & Skov, M. B. (2017). Child-computer interaction SIG: Ethics and values. In G. Mark & S. Fussell (Eds.), *Proceedings of the 2017 CHI conference Extended Abstracts on Human Factors in Computing Systems: CHI EA '17* (pp. 1334–1337). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3027063.3049286

imec. (2019). *imec.AI barometer*. Leuven: Imec. Retrieved from https://www.imec-int.com/drupal/sites/default/files/inline-files/AI-meter.pdf

Information Commissioner's Office. (2019). *Age appropriate design: A code of practice for online services* (No. 20190412). Wilmslow: Information Commissioner's Office. Retrieved from https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf

Iversen, O. S., Smith, R. C., & Dindler, C. (2017). Child as protagonist: Expanding the role of children in participatory design. In P. Blikstein & D. Abrahamson (Eds.), *Proceedings of the 2017 conference on Interaction Design and Children: IDC '17* (pp. 27–37). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3078072.3079725

Iversen, O. S., Smith, R. C., & Dindler, C. (2018). From computational thinking to computational empowerment: A 21st century PD agenda. In L. Huybrechts, M. Teli, A. Light, Y. Lee, J. Garde, J. Vines, . . . K. Bødker (Eds.), *Proceedings of the 15th Participatory Design Conference on Full Papers: PDC '18* (pp. 1–11). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3210586.3210592

Kawas, S., Yuan, Y., DeWitt, A., Jin, Q., Kirchner, S., Bilger, A., . . . Yarosh, S. (2020). Another decade of IDC research: Examining and reflecting on values and ethics. In E. Rubegni & A. Vasalou (Eds.), *IDC '20: Proceedings of the Interaction Design and Children Conference* (pp. 205–215). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3392063.3394436

Kemmis, S., McTaggart, R., & Nixon, R. (2014). *The action research planner*. Singapore: Springer. https://doi.org/10.1007/978-981-4560-67-2

Kinnula, M., Livari, N., Molin-Juustila, T., Keskitalo, E., Leinonen, T., Mansikkamäki, E., . . . Similä, M. (2017). Cooperation, combat, or competence building: What do we mean when we are 'empowering children' in and through digital technology design? In Y. J. Kim, R. Agarwal, & J. K. Lee (Eds.), *Proceedings of the Thirty Eighth International Conference on Information Systems*. Atlanta, GA: Association for Information Systems. Retrieved from https://aisel.aisnet.org/icis2017/TransformingSociety/Presentations/15

Le Dantec, C. A., & DiSalvo, C. (2013). Infrastructuring and the formation of publics in participatory design. *Social Studies of Science*, *43*(2), 241–264. https://doi.org/10.1177/0306312712471581

Le Dantec, C. A., & Fox, S. (2015). Strangers at the gate: Gaining access, building rapport, and co-constructing community-based research. In D. Cosley & A. Forte (Eds.), *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing—CSCW '15* (pp. 1348–1358). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/2675133.2675147

Lievens, E., & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the general data protection regulation. *Computer Law & Security Review*, *34*(2), 269–278. https://doi.org/10.1016/j.clsr.2017.09.007

Lievrouw, L. A. (2006). Oppositional and activist new media: Remediation, reconfiguration, participation. In G. Jacucci & F. Kensing (Eds.), *PDC '06: Proceedings of the ninth conference on Participatory design: Expanding boundaries in design—Volume 1* (pp. 115-124). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/1147261.1147279

Livingstone, S. (2019, January 28). Children's personal privacy online: It's neither personal nor private. *Media@LSE*. https://blogs.lse.ac.uk/medialse/2019/01/28/childrens-personal-privacy-online-its-neither-personal-nor-private

Lobel, A., Granic, I., Stone, L. L., & Engels, R. C. M. E. (2014). Associations between children's video game playing and psychosocial health: Information from both parent and child reports. *Cyberpsychology, Behavior, and Social Networking*, *17*(10), 639–643. https://doi.org/10.1089/cyber.2014.0128

Löwgren, J., & Reimer, B. (2013). The cultural form of collaborative media. In J. Löwgren & B. Reimer (Eds.), *Collaborative media: Production, consumption, and design interventions* (pp. 13–28). Cambridge, MA: MIT Press.

Mainsah, H., & Morrison, A. (2012). Social media, design and civic engagement by youth: A cultural view. In K. Halskov, H. Winschiers-Theophilus, Y. Lee, J. Simonsen, & K. Bødker (Eds.), *Proceedings of the 12th Participatory Design Conference on Research Papers: Volume 1—PDC '12* (pp. 1-9). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/2347635.2347637

Markman, G. D., Siegel, D. S., & Wright, M. (2008). Research and technology commercialization. *Journal of Management Studies*, *45*(8), 1401–1423. https://doi.org/10.1111/j.1467-6486.2008.00803.x

Markopoulos, P., Read, J., MacFarlane, S., & Hoysniemi, J. (2008). *Evaluating children's interactive products: Principles and practices for interaction designers*. Boston, MA: Morgan Kaufmann.

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

McAdam, M., Miller, K., & McAdam, R. (2018). Understanding quadruple helix relationships of university technology commercialisation: A micro-level approach. *Studies in Higher Education*, *43*(6), 1058–1073. https://doi.org/10.1080/03075079.2016.1212328

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy*, *16*(4), 266–275. https://doi.org/10.1111/j.1467-9973.1985.tb00173.x

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. New York, NY: PublicAffairs.

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

Read, J. C., Fitton, D., Sim, G., & Horton, M. (2016). How ideas make it through to designs: Process and practice. In S. Björk & E. Eriksson (Eds.), *Proceedings of the 9th Nordic Conference on Human-Computer Interaction: NordiCHI '16* (pp. 1–10). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/2971485.2971560

Robertson, R., & Allen, P. (2018). Empathy is not evidence: Four traps of commodified empathy. In D. Nafus & T. Rattenbury (Eds.), *EPIC Proceedings* (pp. 104–124). Oregon: EPIC. Retrieved from https://www.epicpeople.org/intelligences

Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*, *20*(2), 127–142. https://doi.org/10.1007/s10676-018-9452-x

Schepers, S., Dreessen, K., & Zaman, B. (2018a). Rethinking children's roles in participatory design: The child as a process designer. *International Journal of Child-Computer Interaction*, *16*, 47–54. https://doi.org/10.1016/j.ijcci.2017.12.001

Schepers, S., Dreessen, K., & Zaman, B. (2018b). Exploring user gains in participatory design processes with vulnerable children. In L. Huybrechts, M. Teli, A. Light, Y. Lee, J. Garde, J. Vines, . . . K. Bødker (Eds.), *Proceedings of the 15th Participatory Design Conference on Short Papers, Situated Actions, Workshops and Tutorial: PDC '18* (pp. 1–5). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3210604.3210617

Steijn, W. M. P., & Vedder, A. (2015). Privacy under construction: A developmental perspective on privacy perception. *Science, Technology, & Human Values*, *40*(4), 615–637. https://doi.org/10.1177/0162243915571167

United Nations. (1989). *Convention on the rights of the child.* New York, NY: United Nations. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

Vandenberghe, B., & Slegers, K. (2016). Designing for others, and the trap of HCI methods & practices. In J. Kaye & A. Druin (Eds.), *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 512–524). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/2851581.2892584

van Dijck, J. (2009). Users like you? Theorizing agency in user-generated content. *Media, Culture & Society*, *31*(1), 41–58. https://doi.org/10.1177/0163443708098245

Viviers, A. (2014). *General comments of the committee on the rights of the child a compendium for child rights advocates, scholars and policy makers*. New York, NY: UNICEF. Retrieved from https://www.unicef.org/southafrica/SAF_resources_crcgeneralcomments.pdf

Wagner, I. (2018). Critical reflections on participation in design. In V. Wulf, V. Pipek, D. Randall, M. Rohde, K. Schmidt, & G. Stevens (Eds.), *Designing socially embedded technologies in the real-world* (Vol. 1, pp. 243–278). Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198733249.003.0008

Wauters, E., Donoso, V., & Lievens, E. (2014). Optimizing transparency for users in social networking sites. *Info*, *16*(6), 8–23. https://doi.org/10.1108/info-06-2014-0026

Yu, J., Stoilova, M., & Livingstone, S. (2018, January 11). Regulating children's data and privacy online: The implications of the evidence for age-appropriate design. *Media@LSE*. Retrieved from https://blogs.lse.ac.uk/medialse/2018/11/01/regulating-childrens-data-and-privacy-online-the-implications-of-the-evidence-for-age-appropriate-design

Zimmerman, M. A. (2000). Empowerment theory. In J. Rappaport & E. Seidman (Eds.), *Handbook of community psychology* (pp. 43–63). Boston, MA: Springer. https://doi.org/10.1007/978-1-4615-4193-6_2

About the Author

Bieke Zaman is Associate Professor and Head of the Meaningful Interactions Lab (Mintlab) at KU Leuven. Her research lies at the intersection of human–computer interaction research and communication sciences. Fascinated by the tech side of social, and the social side of tech, Zaman pursues research programs on Children, Media and Design, Media Convergence in a Digital Society, and Progressive Research and Dissemination Methods.

Media and Communication (ISSN: 2183-2439)

Media and Communication is an international open access journal dedicated to a wide variety of basic and applied research in communication and its related fields. It aims at providing a research forum on the social and cultural relevance of media and communication processes.

www.cogitatiopress.com/mediaandcommunication

COGITATIO