Article

"Privacy Is Overrated": Situating the Privacy-related Beliefs and Practices of Italian Parents with Young Children

Lorenzo Giuseppe Zaffaroni

Università Cattolica del Sacro Cuore, Italy
lorenzogiuseppe.zaffaroni@unicatt.it

Abstract

The widespread surveillance of everyday family life poses threats to parents' and children's right to privacy. Even though considerable research on privacy in families with young children exists, more evidence on the interplay between contextual factors and privacy issues is needed to enrich our understanding of privacy as *grounded* in everyday family life. To this aim, this paper conceptualises privacy as a *situated* and *emergent* phenomenon related to family cultures, socioeconomic background, technological imaginaries, and other significant markers of everyday family life. Drawing on qualitative data from a longitudinal research project with parents of children aged zero to eight, the study shows that privacy risks and threats are mostly associated with the interpersonal context; corporate and institutional surveillance are naturalised within notions of convenience or resignation to big-tech corporations. As technological and surveillance imaginaries influence such a complex web of privacy dynamics, this paper advocates for a situated and contextual approach to family privacy and surveillance in times of datafication.

Introduction

Modern households have become datafied environments where vast amounts of data on parents and children are collected through various internet-connected devices (Barassi 2020; Lupton and Williamson 2017; Mascheroni and Siibak 2021). Accessing digital media positions parents and children as data subjects (Isin and Ruppert 2015; Mascheroni 2018) whose daily interactions with various media enable the pervasive surveillance of everyday family life (Mascheroni 2020). In this context, threats to children's right to privacy emerge as a multifaceted and pressing issue (Livingstone and Third 2017). Despite a wealth of literature on privacy-related practices and beliefs, several areas remain uncharted. Notably, while privacy is framed as an individual responsibility in public discourses (Keen 2022; Mascheroni 2018), further research concerning the diverse and situated beliefs concerning privacy, and the practices aimed to achieve and protect it, could reveal the complex and shifting conditions affecting family life—and, ultimately, the digital rights of family members. To this end, this paper conceptualises privacy as a situated phenomenon—that is, connected to families' cultures, socioeconomic backgrounds, technological imaginaries, and other significant dimensions of everyday family life. By doing so, the study provides a situated understanding of underexplored areas (Stoilova, Nangadiri, and Livingstone 2019) besides interpersonal negotiations (e.g., Berriman and Jaynes 2022), such as family members' interactions with commercial contexts. The paper will also touch upon the institutional context, although to a lesser degree due to a lack of both direct experiences and awareness of its implications in this area among the participating families, given the young age of their children. Furthermore, the paper reports on the less-explored experiences of families with younger children (Stoilova, Nangadiri, and Livingstone 2019), bearing in mind the increased responsibility placed on parents in the early stages of their children's lives.

Zaffaroni, Lorenzo Giuseppe. 2024. "Privacy Is Overrated": Situating the Privacy-related Beliefs and Practices of Italian Parents with Young Children. *Surveillance & Society* 22 (4): 410-427.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

The article draws on qualitative data from a longitudinal research project involving twenty Italian families with children aged zero to eight, offering insights into how social imaginaries about technology, media use, social pressures, and the dynamics of everyday life play a fundamental role in privacy dynamics. Adopting Stoilova, Nangadiri, and Livingstone's (2019) threefold categorisation of privacy contexts, the paper focuses on privacy-related beliefs and practices across the interpersonal, commercial, and institutional domains by addressing a set of research questions: What privacy-related practices do parents engage in? [1] What privacy-related beliefs are most valued by parents? How do these privacy-related practices and beliefs interplay with the unfolding of various interconnected media practices, social pressures, and norms, as well as technological imaginaries, in everyday family life?

The results show that families have a varying but still limited awareness of privacy risks and threats related to the use of digital devices and online interactions. Italian families mostly show a range of concerns about their children's privacy that are related to the interpersonal context, including the protection of personal data, online safety, and safeguarding media exposure. At the core of the complex web of family privacy lie social and cultural factors, influencing the emergence and negotiation of privacy-related practices within everyday family life. The discussion will highlight the value of situating privacy-related beliefs and practices into the contexts and histories in which they evolve, revealing the complex challenges of datafied parenthood and childhood.

Parents and Children's Privacy in Times of Datafication

Extant scholarship points to various factors that influence how family members negotiate privacy against the background of intensified datafication. In family life, privacy issues emerge in the context of the increasing mediatization of parenthood (Damkjær 2018) as various media practices have become the norm and a means for parents to achieve social recognition while feeding the logics of "surveillance capitalism" (Zuboff 2019) and datafication (Couldry and Mejias 2019; van Dijck 2014). One prominent area of study is sharenting, a practice parents engage in by sharing their children's personal information and content on social media platforms (Blum-Ross and Livingstone 2017). Research shows that parents navigate conflicting norms and expectations, calibrating the need to perform online parenting through increased online exposure while at the same time aiming to protect children's data by enforcing their individual responsibility (Mascheroni 2018). In the Italian context, extant research on sharenting reveals its gendered and generational features (Mascheroni et al. 2023): Italian mothers in the eighteen to thirty-four age group are those more prone to share on a regular basis. Sharenting is thus configured as a "mandatory" practice associated with parents' needs for self-representation and recognition (Mascheroni et al. 2023). However, only a few parents ask their young children (aged zero to eight) for permission.

Furthermore, in studying the privacy boundaries emerging from smartphone adoption among Italian adolescents, Mascheroni (2014) finds that conflicting privacy-related discourses are influenced by various cultural factors associated with different parenting styles—such as parents' own values and domestication of household media. In addition, while studies on the Italian context reveal that adolescents (aged thirteen to seventeen) face more privacy risks than children aged nine to twelve, such as the misuse of their personal data (Mascheroni and Olaffson 2018), more research that contextualises datafied relations in Italian families with young children (aged zero to eight) is needed. In this respect, an Italian survey (Zaffaroni, Amadori,

[1] The primary focus of this paper concerns parents' accounts of privacy-related beliefs and practices given that parents of very young children guide and often act on behalf of their children when it comes to data sharing (Chaudron et al. 2018; Kumar et al. 2017). While focusing on parents, the analysis also acknowledges the perspectives of older children and older siblings in our sample. Despite various studies acknowledging how adults often underestimate how aware and capable children could be in respect to privacy issues (Marwick and boyd, 2014, Üzümcü, 2023), the few empirical studies on children under age seven (see Livingstone, Stoilova, and Nandagiri 2019) observe how very young children are often unaware of privacy concerns (Kumar et al. 2017).

and Mascheroni 2022) shows that only 13% of parents of children aged zero to four asked their children's permission before uploading content depicting them, compared to 36% of parents of children aged five to eight. These results reveal that parents might hold different perceptions of young children's capacity to decide on their online presence. The issue of consent in privacy negotiations (or lack thereof) is central, as research reveals parents often dismiss the privacy implications associated with sharenting, thus undermining children's digital rights (Barnes and Potter 2019; Lipu and Siibak 2021).

Relatedly, research on tracking technologies, such as surveillance cameras (Mäkinen 2016), parental controls, and monitoring apps, also reveals how parent exert both control and care through forms of "intimate surveillance" (Leaver 2017) and "caring dataveillance" (Lupton 2020). Yet, these practices, while presented as solutions to digital parenting in what is deemed "transcendent parenting" (Lim 2020), have the potential to increase the privacy risks of all family members (Ali et al. 2020).

While parents show more awareness of commercial privacy breaches (Bietz et al. 2019), young children seem mostly concerned with privacy violations relating to the social and interpersonal sphere (Livingstone, Stoilova, and Nandagiri 2019). A possible explanation lies in their partial or limited understanding of how data collection works, including its social consequences (Pangrazio and Selwyn 2019). In this respect, parents of younger children act as mediators and hold different positions informed by their parenting styles (Dias and Brito 2020; Mascheroni 2014). Growing evidence points to the acceptance, in various social discourses, of sacrificing privacy for safety (Hasinoff 2017; Marx and Steeves 2010). While younger children might not always perceive these practices as privacy-intrusive, negotiations between parents and young children are still an important part of everyday family life (Berriman and Jaynes 2022; Dias and Brito 2020). Besides, children can explicitly express the need to take part in negotiations around privacy boundaries (Sukk and Siibak 2021).

Privacy as Situated and Contextual

Contextual privacy models emphasise variations in privacy constructs and practices across cultures, time, and technological developments (Nissenbaum 2010). Specifically, privacy in the context of family life is linked to the (shifting) daily media routines, affective networks (Das et al. 2023), life trajectories (Hodkinson and Brooks 2023), and power dynamics between parents and children. Furthermore, privacy is also contingent on the expectations placed upon parents as "good" mediators and mentors (Livingstone and Blum-Ross 2020).

Drawing on Nissenbaum's (2010) view of privacy as a matter of "contextual integrity," Stoilova, Nangadiri, and Livingstone (2019) identify three key privacy domains: interpersonal (e.g., privacy relations with other individuals), institutional (e.g., with schools), and commercial (e.g., with companies). Each domain involves distinct power dynamics and regulatory approaches, posing different conditions and risks to privacy negotiations in everyday life. Furthermore, Stoilova, Nangadiri, and Livingstone (2019) propose to distinguish between "given" data, "data traces," and "inferred data" (or metadata). In this respect, it is crucial to understand how parents form algorithm literacies around different types of data because, "as digital data become more ubiquitous to everyday life, it is also becoming increasingly difficult for non-specialists to define and understand" (Pangrazio and Selwyn 2019: 420). Furthermore, everyday relations with algorithms are influenced by cross-media and multi-platform life (Das 2023). As parents and children increasingly use the internet on multiple platforms, their skills may be fragmented and varied across platforms and devices. Besides, algorithms themselves perform differently depending on the platform and the user that interacts with them (Mehrnezhad 2020).

In addition, social imaginaries about technology and surveillance (Lyon 2018) matter in establishing the legitimising grounds for various privacy-related practices. With the shift to surveillance as a culture, surveillance imaginaries do not "act" on individuals; rather, individuals contend with surveillance

imaginaries, appropriating, negotiating, or opposing them (Lyon 2018). Parental practices, such as "caring dataveillance," cannot be properly analysed without taking into account how technological and surveillance imaginaries are rationalised in relation to dominant parenting values (Sukk and Siibak 2021). For instance, tracking technologies are associated with a sense of reassurance (Brown et al. 2007) that is exploited by tech companies capitalising on parents' growing anxieties (Leaver 2017). Thus, competing interests and evolving roles and responsibilities all factor into how privacy is conceptualised and enacted. In other words, privacy is interwoven with the social and cultural fabric of everyday family life.

Methods

The paper draws from qualitative data collected within the longitudinal mixed-methods research project DataChildFutures (2020–2023), which focused on the datafication of childhood and family life. The research team recruited the participating families through snowball sampling, asking colleagues and acquaintances to disseminate a leaflet summarising the research project in their workplaces and on social media platforms (i.e., parent Whatsapp or Facebook groups). Our criteria for recruitment included families residing in the Milan metropolitan area who had at least one child aged zero to eight, as this age group is underrepresented in studies on children's privacy and the datafication of childhood (Stoilova, Nangadiri, and Livingstone 2019). Our final sample consisted of twenty families that are diverse in terms of socioeconomic status, media ensemble, and family composition (see Table 1). One "selected" child was identified for each family. In families with multiple children within the desired age-range, the researchers let parents decide the designated child. Older siblings were included in the study as active participants. Before data collection, parents were asked to read and sign a consent form for themselves and on behalf of their children. The consent form was prepared by the lead researcher of the project and approved by the ethics committee of Università Cattolica del Sacro Cuore in Milan, Italy.

The study included three waves of data collection: November–December 2021; April–May 2022; and November 2022–January 2023. All the participant families took part in the three waves of data collection, except for Family 1, who dropped out of the study before our second meeting. The research team comprised three members: a full professor as lead researcher, a postdoctoral researcher, and a PhD student. In each wave, two researchers conducted face-to-face interviews in the participants' homes. Strict adherence to the COVID-19 safety protocols was prioritised each time. In the first interview, we asked children to partake in a toy and digital media tour (Plowman and Stevenson 2013) in which they showed their favourite (digital) toys and devices, providing relevant information on which (digital) practices they engaged in, where, and with whom while developing trusting relationship with the researchers. These preliminary data informed our understanding of the routines and habits of the families and revealed aspects that were further probed in the following interviews. Meanwhile, and preferably not in the presence of the designated children nor siblings, the other researcher interviewed the parents about the media practices of the family, their mediation strategies, their imaginaries concerning technologies, and their privacy-related beliefs. Initial interviews with parents identified their perceptions of privacy and awareness of digital risks in relation to the broader dynamics of daily life.

The second wave included a brief recap where some issues were reiterated and potential adjustments were recorded. Both parents and children took part in the conversation. We then proposed a map-drawing method (Watson, Lupton, and Michael 2022) to the parents (but willing children could also do it on their own) to foster reflection and discussion on the domestication of digital media. The second meeting allowed us to contextualise privacy in relation to broader dimensions of mediatised family life, including temporal-spatial dynamics, communicative practices, and parents' concerns and hopes regarding the presence of media in their children's lives.

During the third and final meeting, the results from the first and second waves were presented to the parents and children through a network map created by one of the team members (Amadori and Mascheroni 2024)

by drawing on previous interviews and observations. The map shows two types of nodes, namely family members (parents and children), who are connected to owned and shared digital devices. In the map, different colours indicate individual device usage while the varying thicknesses of the connections indicate how meaningful each individual's relationship with a device is. The maps were employed in the third interview in order to stimulate the participants' reflexivity and touch again upon potentially underexplored areas.

The transcribed interviews were anonymised (by replacing participants' names with made-up ones they were willing to create or choose) and analysed using Constructivist Grounded Theory (CGT) (Charmaz 2014). CGT conceptualises data collection and analysis as iterative processes that should be coupled as soon as fieldwork begins. CGT enables the analysis of meaning-making processes as situated and contingent upon the experiences of interviewers and interviewees, as well as the evolving trajectories of research (Charmaz 2014). Initially, the team of three researchers independently conducted line-by-line coding on a single transcript and then compared the resulting codes to identify similarities and discrepancies. When an agreement was met, further rounds of coding (on Wave 1 data) allowed for broader codes to be identified. Based on this, the researchers progressively constructed a code sheet made of higher-level thematic codes (i.e., "privacy-related practices," "privacy-related beliefs," and "technological imaginaries") that were applied to include previously identified sub-processes and discursive patterns. The common shared code sheet was used to guide the second and third phases of analysis to guarantee that all researchers focused on all areas of interest while coding the interview transcripts independently. Before aggregating all files into a shared MaxQDA database, the lead researcher checked for accuracy and consistency across all analyses. The interview excerpts provided in this paper were translated into English by the author of the article.

Table 1: *Participating Families*

Family Number	Parents (age, nationality)	SES	Selected Child	Siblings	Devices
Family 1	Mother (39, Italian); Father (43, Italian)	High	F, 5		13
Family 2	Mother (37, Italian); Father (38, Italian)	Medium	M, 4	M, 1	10
Family 3	Mother (42, Italian); Father (48, Italian)	Medium/Low	F, 3		10
Family 4	Mother (38, Russian); Father (38, Italian)	Medium	F, 4		13
Family 5	Mother (37, Belgian); Father (45, Italian)	High	F, 6	M, 3	4
Family 6	Mother (43, Italian); Father (43, Italian)	Medium	M,5		13

Family 7	Mother (42, Italian-Swiss); Father (39, Italian-French)	Medium	M, 5	F, 2	6
Family 8	Mother (41, Italian); Separated	Medium/High	M, 5		10
Family 9	Mother (41, Italian); Father (42, Italian)	High	M, 7	M, 18m; M, 3; M, 6; F, 10; F, 13; F, 14;	10
Family 10	Mother (40, Italian); Father (44, Italian)	Medium	M, 7		14
Family 11	Mother (34, Moroccan); Father (46, Italian)	Medium/Low	M, 6	M, 8	12
Family 12	Mother (38, Italian); Separated	Medium	M, 6	F, 10	17
Family 13	Mother (41, Italian); Father (49, Italian)	Low	M, 6		12
Family 14	Mother (40, Italian); Father (40, Italian)	Medium	F, 7	M, 3; M, 12; F, 10	14
Family 15	Mother (42, Italian); Father (42, Italian)	Medium/Low	M, 6		12
Family 16	Mother (40, Italian); Divorced	Medium	M, 7	M, 5	11
Family 17	Mother (37, Moldavian-Russian); Separated	Low	F, 8		9
Family 18	Mother (40, Italian); Father (41, Italian)	Medium-High	F, 8	F, 10	21
Family 19	Mother (53, Italian); Father, (58, Italian)	High	M, 5		15
Family 20	Mother (49, Italian); Father (49, Italian)	Medium	F, 8	F, 11	11

The total number of devices include laptops and desktop computers, tablets, smartphones, game consoles, smart and traditional TVs, eBook readers, connected toys, smart speakers, and smart home appliances.

Privacy-related Beliefs and Practices across Different Privacy Contexts

With the term "privacy-related practices," this paper designates the broad set of practices relating to negotiating, achieving, and protecting privacy across the three contexts—interpersonal, commercial, and institutional—identified by Stoilova, Nangadiri, and Livingstone (2019). The term references Stoilova, Nangadiri, and Livingstone's (2019) systematic evidence mapping of research on children's privacy, which distinguishes, for analytical reasons, studies focusing on the privacy-related practices of family members from those focusing on the privacy-related values and beliefs about the internet. In a similar vein, for analytical purposes, this paper identifies—under the term "privacy-related beliefs"—the set of values, motivations, and conceptualisations (Keen 2022) concerning how (and to what extent) privacy can be achieved and protected, as well as the awareness about the sources of risk and the potential social consequences connected to sharing (different types) of data.

Table 2 provides an overview of the privacy-related beliefs and practices held by the parents across the three privacy contexts identified by Stoilova, Nangadiri, and Livingstone (2019). The results show that common definitions of privacy are shared among most participants—specifically concerning the interpersonal level and mostly contingent on the "given data" provided by parents. Furthermore, parents' shared concerns highlight the need to safeguard proprietary information from unwanted scrutiny. However, the intensity of concerns and the divergence in privacy-related practices and beliefs vary across different families depending on the emergent and situated nature of privacy—that is, depending on the relationship between privacy-related beliefs and the wider fabric of mediatised family life. The detailed findings below are also structured along the threefold framework by Stoilova, Nangadiri, and Livingstone (2019).

Table 2: *Privacy-related Beliefs and Practices across Contexts*

	Interpersonal	**Commercial**	**Institutional**
Privacy-related beliefs	Strong desire to protect privacy against unknown others. Desire to protect proprietary data.	"Nothing to hide." Ignoring the importance of data traces and inferred data. Minimising the social consequences of datafication. Exhibiting consensus apathy (Keen 2022).	Trust in school as an institution. Little perception of risks in the context of educational apps.
Privacy-related practices	Frequent aversion towards sharenting. Enacting surveillance and caring dataveillance practices towards family members.	Willingness to share identifying information on oneself. Adopting ineffective strategies to circumvent corporate surveillance.	Sharing information on children if schools require it. Using apps for educational purposes.

	Using social media with private profiles as a protective strategy.	Little control and agency on privacy settings.	

Interpersonal Privacy

Interpersonal privacy is based upon the need to balance openness and visibility against the intimacy of family life across different social boundaries. Such tension between public scrutiny and intimacy concerns unknown others—to a greater extent in the context of social media—as well as members of the extended family, such as grandparents, and other personal networks (e.g., schoolmates' parents). Various parents revealed having a shared understanding of sharenting as a practice that poses challenges to the daily negotiation of privacy boundaries (Marwick 2012); therefore, many develop coping strategies that are compatible with the conduct of daily life amidst pressing commitments and demands. For example, grandparents often express their desire to participate in their grandchildren's lives in ways that are increasingly mediatised, and therefore difficult to manage:

> **Interviewer 2:** And the grandfather, on the other hand, I remember that you had agreed there too. Does he continue [to take pictures]?
>
> **Lisa:** He continues but without posting pictures. Yes, maybe it happened on his birthday, that there were some pictures, but that's OK. He's not one to [do it]... fortunately, in fact. (Family 10, Wave 3)

Intra-family privacy negotiations evolve dynamically based on several adjustments (and exceptions) that, as in the case of Family 10, impose restrictions on undesirable behaviour. Parents usually oppose non-consensual sharing by others since it could not only undermine children's emerging autonomy (Livingstone and Third 2017) but also their authority as parents. By restricting sharenting, parents reinforce their position of control over how children's mediated representations are created and disseminated (Moser, Chen, and Schoenebeck 2017).

Often, parents discuss their values related to privacy with friends and fellow parents as part of the wider discussions and sense-making around parenting that arise in day-to-day occasions, such as picking up children at school. During these occasions, parents' views of privacy are informed by comparisons between themselves and other families. For example, parents evaluate the different implications of data sharing inside and outside the boundaries of the family by referring to anecdotes or significant stories shared by other parents:

> **Carlo:** No, for example [there was] a really strange situation yesterday. We were in the little square in front of the school. I was playing with [my son, 3-y.o.] and his mates, and [my daughter, 6-y.o.] went with a couple of mates and the mum of one of them, who made TikTok videos, the mum.
>
> **Interviewer 2:** This mother made videos....
>
> **Carlo:** Well, it seemed wrong to me. Then it is difficult to say [something] in front of them. But maybe I have to find a way to talk to her. We'd prefer not to have this, neither making a video doing a mindless dance, if I can use the expression, nor the fact that this stuff here then circulates without any kind of control by us. As they say, "the right to be forgotten." (Family 5, Wave 3)

As this excerpt shows, parents discuss the rules and routines of other known households using morally charged terms, contrasting the dispositions embedded in other family media cultures and habits with their own.

Importantly, when negotiating interpersonal privacy rules with other families, parents usually resort to justifications related to the principles of permission-seeking and respecting children's evolving preferences (Moser, Chen, and Schoenebeck 2017). These values underlying privacy bargaining, however, seem to be most mobilised when tensions or confrontations involve public visibility—i.e., the example above, when another parent wishes to include one's children in a publicly visible social media post. In the context of private family life, children's agency more frequently takes a back seat, since parents often do not offer their children active opportunities for negotiation due to their young age. Instead, parents set the rules relating to the online presence of their children by acting on their behalf. Despite this, interpersonal privacy risks are still recognised by most parents in the study.

Many families demonstrate some awareness about the implications of image sharing, realising that images sent through different channels—and, therefore, through different interpersonal contexts—involve different degrees of scrutiny and agency. For instance, Rita, a separated mother, asked her sister to refrain from posting pictures of her two children on social media, yet she engages in sharenting herself via WhatsApp status updates since "clearly, they are internal contacts." Parents often feel more secure when engaging in interpersonal communication through channels perceived as "closed" since they believe most risks associated with children's privacy primarily arise from unsolicited interpersonal contacts. Parents with more digital skills, conversely, can articulate different scenarios, showing an implicit awareness of "networked" privacy (Marwick and boyd 2014). Carlo, a clinical data strategist, claims that images (such as his children's pictures, which he avidly takes on every travel occasion) leave traces that are difficult to control when shared with unreliable others, "One thing is when you want to send a picture to someone else. But not the stuff that sticks around, and that you never know what fate it might have; one does it with the best of intentions, and then... things outlive one's intention" (Family 5, Wave 1). Digital data, being persistent and searchable, require parents to take a stance against the collapse of context and previously accepted boundaries (boyd 2014). Yet, while Carlo points to how sharing amplifies outcomes that are impossible to foresee or retract, interpersonal concerns (e.g., the lack of intent on behalf of other subjects) overshadow how privacy harms are connected to online platforms and their security issues.

Alternatively, families that frequently share photos on social media seem to underestimate how relevant children's data are and how permanent sharenting can be (Debatin et al. 2009). In Family 4, parents dismiss how children's "given off" data and metadata are generated daily, which they believe they retain ownership of while posting on social media:

> **Ludmilla (mother):** After all, she's a four-year-old girl, it is generic data. With photos, it's a different story, there you may say that....
>
> **Filippo (father):** We do post, I mean....
>
> **Ludmilla:** Yes, but it's not that we give out photos, you know, not that.
>
> **Filippo:** No, we post them on social media. (Family 4, Wave 2)

Different levels of sensitivity around different types of personal data inform parents' beliefs towards privacy. Filippo focuses more on the public aspect of posting on social media, while Ludmilla is more concerned about directly providing the rights to her daughter's personal data to other individuals (compared to Instagram as a platform). This excerpt shows nuanced perspectives on privacy as it relates to audiences and beliefs in data ownership: neither parent refers directly to platforms' data practices, focusing more on

their own sharing behaviours and their reception. The interpersonal lens in conceptualising privacy obfuscates the other forms of data creation underlying (social) media practices.

As interpersonal privacy takes centre stage in daily negotiations, social media is the site where more privacy-protective strategies are implemented. Children with more access to devices and social media accounts are persuaded by peers to post content online; in response, parents strive to find a balance between allowing access to services that seem socially relevant to their kids and taking into account the risks that often come with platforms not designed for children. Parents can set up private, "passive" accounts as shields from potential threats posed by unknown others or resort to heavier monitoring, while a few take a more enabling approach. In Family 12, where mother Rita is willing to discuss online risks with her children, older daughter Giulia (ten) learns about privacy-protective strategies from her schoolmate, and thus hopes to negotiate content creation on TikTok with her mother:

> **Giulia (10-years-old daughter):** I watch TikTok, but I can't create them [with an annoyed tone] [....] There's a classmate of mine...[...] [Her parents] gave her a mask for Christmas, I think, so she can do dances....
>
> **Interviewer 2:** Is the mask used for filters...or a mask to make....
>
> **Giulia:** …to hide her face [in the videos]. (Family 12, Wave 1)

Contextual factors like age appropriateness, peer influences, and informal talk play a central role in everyday negotiations around young children's online privacy, in addition to individual dispositions established by parental mediation. In particular, interpersonal privacy is situated within, and develops in relation to, the narratives, norms, and social trajectories that characterise each family. In this respect, the acceptance, negotiation, or rejection of technological and surveillance imaginaries are key markers in establishing variations in privacy-related beliefs and practices. For example, Ludmilla (mother, Family 4) discussed installing security cameras in her mother's house to monitor her remotely for safety concerns. In recounting this, she pointed to socially acceptable preoccupations legitimising surveillance needs within the family:

> **Ludmilla:** I downloaded the app and installed cameras at my mother's house.... So, we are spying every now and then; we introduced this as a...novelty. Every now and then we talk to grandma, we're like [voicing her daughter]: "Grandma! Good morning!"
>
> **Interviewer 1:** Does she hear you from this app?
>
> **Ludmilla:** Yes, I downloaded the camera app. Because she hasn't been well, so I put the…the camera.
>
> **Interviewer 1:** For safety.... Does she live alone?
>
> **Ludmilla:** No, with my father. But, still.... (Family 4, Wave 1)

"Surveillance equipment" has transformed the way families can effectively manage care even when physically separated (Mäkinen 2016). Yet, such instances of "caring dataveillance" lean onto the commercialisation of parental anxieties, be they projected towards grandparents or children alike. Ludmilla's tone is playful, as she feels the need to create a high-spirited arrangement with her daughter, which further naturalises this practice as part of their daily routine. Surveillance cameras thus introduce new dynamics of co-presence at the expense of the complex entanglements of data being produced on all family members involved. While technologies play a role in intergenerational privacy negotiations due to the new

technologically afforded responsibilities they introduce, families can coexist with new intrusive technologies if they are accepted as benign.

Furthermore, the findings highlight that device sharing and the disruption of privacy boundaries are increasingly emerging in the everyday management of devices. Parents who gift used devices to children, or who let children use shared devices with one common account, contend with complex layers of privacy settings that are often out of their control. For example, many parents do not factory reset their devices before giving them to their children, so the data from their use still remain in them. The implications of device sharing in terms of family members' interpersonal and commercial privacy are often made invisible both by the "opacity" of networked privacy infrastructures (boyd 2014) and by the situated interactions and dispositions within each family. In Family 13, Pamela, a tech-savvy mother, reports her child makes intensive use of the family tablet so that it is, in practice, "his" tablet. During unsupervised use, the child has left comments under YouTube videos while being logged in to Pamela's Google account:

> **Pamela:** […] I mean, the fact that he leaves a "like" doesn't bother me that much, it's just that he leaves it under my name, because actually the account is in my name.
>
> **Interviewer 2:** Ok.
>
> **Pamela:** Yeah, that bothers me. (Family 13, Wave 2)

The blurred ownership and control of devices influence the production of personal digital traces in processes of self-presentation and self-disclosure online. Interestingly, Pamela is not concerned with his son leaving data traces. Instead, Pamela is troubled by her personal involvement via identifying details provided under her online name. Pamela's response indicates how intra-family device sharing can undermine individuals' privacy preferences and individual authority, not only because children (and sometimes parents) cannot control account preferences but also because technologies themselves increasingly afford new forms of visibility and agency that impose constant user-identification.

Commercial Privacy

A range of views on commercial data collection emerged from the study, from resignation towards personalised advertising to less frequent but proactive attempts at limiting tracking. Some parents express concern over children's data being collected online, but many feel children's data have little value to companies. Many parents do not limit the use of platforms based on extensive extraction of data (i.e., YouTube) due to privacy reasons, as they ignore the implications of how algorithms and (various forms of) data profiling work (Pangrazio and Selwyn 2019). In this scenario, families balance data collection with the perceived benefits of technologies and services. In Family 4, both parents declare their willingness to share personally identifiable information for convenience:

> **Filippo (father):** We think privacy is a bit overrated, that is. If one has nothing to hide, why care about privacy, right? I mean, what you do, what you buy, what you eat, what your habits are.... I mean, it's inevitable anyway [....] You deprive yourself of all the benefits of using technology, for what? Do you think that you harm corporations, that you deprive them of your individual data? You are an individual among billions, and so...to deprive who knows whom of data. Whatever, I would never deprive myself of any comfort provided by technology! (Family 4, Wave 2)

Views like Filippo's downplay privacy concerns by portraying data collection as inescapable once technologies and their benefits are incorporated into daily life—and, thus, into his daughter's life. This fatalism ("it's inevitable anyway") is coupled with an emphasis on the perceived "benefits" of services and the conveniences made possible through platforms and data flows. Under this imaginary of "surveillance

realism" (Dencik 2018), users who have "nothing to hide" envision themselves more as grateful individuals meant to embrace such advantages rather than critical agents capable of envisioning alternative models. In Family 2, Petra articulates a similarly resigned, yet conditional, acceptance of commercial surveillance based on her perceived control and preference for filtered services, prioritising benefits over the (overlooked) consequences of ubiquitous tracking:

> **Petra:** Google must be listening to us. I know it does, but I don't care, in the end I don't say anything bad. Do you want to trace me? I feel like I don't say anything secret. The day I come up with a plan to rob a bank I'll turn it off anyway [laughs]. If it helps to...send me targeted content. [...] In the end, they'll just spam me with adverts one after the other anyway. At this point, I'd rather have them sent out to me based on my interests. It's better than having them about absurd things like they used to do before, isn't it? (Family 2, Wave 3)

While similarities with the previous excerpt (Family 4) are evident, this statement reveals that the acceptance of commercial surveillance as inevitable and even desirable can be aligned with different and even incompatible world views. During the interviews with Family 2, Petra discusses being concerned about advertising's ideological influence on her children via TV, which they do not own. Overall, Petra tends to provide her children with intellectually stimulating offline activities that align with her middle-class values and high cultural capital. Given this background, Petra would be expected to be more wary of personalised ads. Interestingly, however, her dismissal of privacy concerns might partly stem from the acceptance of algorithmic personalisation, which makes targeted advertising seem less objectionable by "optimising" and "filtering" out what is deemed less culturally valuable. That is, advertising that is more aligned with her cultural interests and parenting style.

Some families demonstrate varying degrees of literacy and control over different types of data in the commercial context. In particular, only a few parents can point out the depth and accuracy that companies exert in extracting data even from from occasional users:

> **Carlo (father):** [I do] the most basic use [of YouTube], without having...[an account]. Then I guess YouTube is then like everything else, they have a perfect profile of me, they know...they know what...what I search for....
>
> **Interviewer 2:** Yeah.
>
> **Carlo:** I don't even have to do that much tinkering; it goes out almost automatically. (Wave 2, Family 5)

While limiting the use of YouTube for himself and, more starkly, for his son and daughter, he has already framed resistance as "useless" due to the seemingly "omniscient" power of data extraction. In our broader conversations with Carlo, he reveals that his international work experience informs his worries. His American colleagues, also parents, alerted him against the subtle commercial interests and strategies employed by big platforms, such as Google. Yet, Carlo's refusal of technology (his family is the least media-rich) mostly stems from his anxiety about screen time as a form of "addiction" and his belief that children's lives are "polluted" by marketing strategies. Carlo's one-size-fits-all solution is thus encouraging outdoor activities and alternative forms of play that are compatible with an "ascetic" (Mascheroni 2023) refrain from technology.

Conversely, a few families are more proactive in limiting the scope of data collection. However, their efficacy is generally based on a limited understanding of how data collection works, as well as the belief

that they can exert enough control on their privacy by providing incorrect data through obfuscation techniques (Pangrazio and Selwyn 2019):

> **Samuele (father):** [...] I seem to remember that I put in some random data in Roblox at the end, and maybe my e-mail address that I don't use. So, I mean, it's not like they can retrieve that much...that much data pertaining to [our son] Edoardo, because [...] I just made up the data. So, it's not a paid app, I don't have anything, so....
>
> **Interviewer 1:** Because you still have to make an account, though.
>
> **Samuel:** I think so, that you have to make the account, but, again, it's the data that I put in.... (Family 15, Wave 2)

Samuele emphasises his agency while engaging in casual efforts of "data obfuscation" (Brunton and Nissenbaum 2016). At the same time, however, he disregards the generation of metadata based on his son's interaction with Roblox and its underlying software infrastructure. Scattered "data tactics" do not necessarily translate to "data reflexivity" (Pangrazio and Selwyn 2019)—i.e., understanding the real impacts in the long run. Often, the main privacy concerns centre on "direct" harms like identity theft rather than the social consequences of datafication:

> **Ludmilla:** But then I don't, I've never quite understood exactly how they can harm, in the end, the....
>
> **Filippo:** The users?
>
> **Ludmilla:** The users, the data thing. Yes.
>
> **Filippo:** Unless we're talking about cases of fraud, but that's another matter, that's a crime [...]. (Family 4 wave 2)

In this respect, the opacity of algorithms serves as a backbone of constant data harvesting since it does not provide the individual with meaningful transparency or user agency. This condition, coupled with parents' trust in data anonymisation as an effective strategy, as well as impersonal or even benign corporate motives (reflected in the previous excerpts), further marginalises individual capacities for contextual privacy (Nissenbaum 2010).

Institutional Privacy

This section touches upon the limited discussions regarding institutional privacy, particularly in schools and regarding the use of educational apps by children. In this respect, the interviews show that the rapid datafication of education creates new circumstances for children to interact with platforms and services, raising intricate privacy concerns.[2] The interviewed parents express having a collaborative and trusting relationship with schoolteachers, which supports the integration of new practices. Parents see teachers as responsible individuals who manage their children's visibility and privacy in the school context. As a result, parents tend to equate their priorities in terms of privacy with the unfolding of teacher-parent relations through an interpersonal lens:

> **Rita (mother):** His teacher was very precise, she made two CDs, with two videos: one with [our son] Davide's face to give [us], and one without Davide's face to share with

[2] While discussions with parents do not tap into institutional privacy definitions that fit within Stoilova, Nangadiri, and Livingstone's (2019) categorisation, the examples still inform how data relations with school institutions often overlap with (or are overshadowed by) parental priorities in terms of interpersonal privacy.

> other parents, because, at that point, the moment the video is in the hands of another parent, you no longer control where it goes. (Family 12, Wave 2)

Similarly, Martina (Family 3) discusses consenting to the kindergarten's photo-sharing app, showing limited knowledge of, and likely limited interest towards, the app's privacy arrangements. Instead, Martina critiques the loss of a teacher-parent relationship due to the photo-sharing app, indicating that privacy-related practices are framed in interpersonal terms even if contextualised within means of digital participation:

> **Martina (mother):** [...] In the kindergarten where she used to go, there was an app that allowed us to see photos of the day. [...] It's called Kindertap, some kindergartens have it. They send you some...pictures and videos of the kids. With pros and cons, in the sense that it limits....
>
> **Interviewer 2:** Yes....
>
> **Martina:** …a lot building up a relationship with... with the teachers, because you... you settle for the picture that shows your child's painting, so you know that she painted that day. (Family 3, Wave 2)

Discussion and Conclusions

This study shows that privacy-related beliefs and practices within datafied family life emerge and are situated in different everyday life experiences and relationships, socioeconomic backgrounds, family cultures, technological imaginaries, and media ensembles. While parents in our sample often share a sense of resignation about privacy, this research uncovers a nuanced set of situated experiences that provide valuable insights into understanding privacy in context.

By differentiating between the interpersonal, commercial, and institutional contexts (Stoilova, Nangadiri, and Livingstone 2019), the study shows how privacy-related beliefs and practices relate to different domain-specific expectations. Echoing previous findings (Keen 2022; Steijn and Vedder 2015; Stoilova, Nangadiri, and Livingstone 2019), parents mostly adopt privacy constructs that relate to the interpersonal dimension and focus on given data. Interpersonal privacy negotiations are influenced by (and in turn inform) different parenting cultures, showing tensions between the desire to share online (matching the ideals of good parenting) and the desire to protect children from online risks (Mascheroni et al. 2023). Similarly, caring dataveillance enables new forms of interpersonal surveillance, eroding pre-existing interpersonal privacy boundaries. As Lyon (2018) points out, surveillance culture involves people actively accepting the need to monitor others—which in turn influences how people think about surveillance. The findings show how the acceptance of surveillance technologies is grounded in techno-optimistic imaginaries that might exclude other subjects from privacy negotiations, such as grandparents.

Concerning the commercial contexts, parents show different degrees of awareness and critical capacities that relate to contextual factors, such as digital skills and literacy, parenting culture, and, importantly, the acceptance of technological imaginaries. Techno-optimistic imaginaries simultaneously legitimise the usefulness of profiling and inhibit efforts to negotiate and control data at the household level. Drawing on Das' (2023) useful categorisation of algorithmic literacy, our findings highlight that, while interviewed parents are "aware in principle," they dismiss the social implications of data relations with companies so that, albeit with some exceptions, "they have learned to live alongside algorithms, without significant changes to their own practices" (Das 2023: 25). Thus, families underestimate—and sometimes purposefully overlook—how behavioural data extraction and third-party data sharing may pose risks to decisional privacy (Keen 2022) and self-determination (Lutz and Hoffmann 2017). A transactional attitude (Das 2023) underlies the exchange of privacy (considered as limited to proprietary data) for convenience.

While parents exercise their responsibility in regulating media access, relevant factors should be considered in analysing privacy-related beliefs and practices. Among these, the pressing demands of connection imposed on families, and the popular idea that technologies might be a resource to children's pathway to "success" (Livingstone and Blum-Ross 2020), play a central role. Adopting new devices, services, and platforms means guaranteeing a form of digital participation for the family while at the same time managing privacy risks individually (van der Hof 2016).

Generally, families that are inattentive to commercial privacy seem to show a greater resignation to surveillance realism (Dencik 2018). This is reflected in a lack of attention or care towards consent, which Keen (2022) highlights with the term "consent apathy," rather than genuine fatigue aroused by the constant demands of technology. As importantly, by dismissing the broader implications surrounding commercial surveillance, parents do not engage in the same degree of discussion and reflection on algorithmic profiling in the presence of very young children. Conversely, parents are more prone to discuss interpersonal privacy risks by drawing upon experiences that children or other families shared with them.

Again, contextualising these pressures within families' cultures and technological imaginaries provides a more nuanced understanding of parental privacy-related practices. For instance, the acceptance of surveillance displayed by techno-optimist families could partly stem from their socioeconomic background as wealthy, middle-class families with ample access to media and technology. As media-rich families, they are more accustomed to the convenience of networked connectivity over critical privacy concerns. Their economic capital gives more room to overlook privacy costs and regard data as currency in exchange for services. These considerations ultimately align with the idea that technological imaginaries, especially "benign" ones, could contribute to the normalisation of surveillance, as parents (such as Family 4, during our second interview) tend to support the idea that technical risks are separate from social ones, and are thus minimised (Keen 2022).

Furthermore, the study reveals the importance of understanding the levels of knowledge, agency, and skills that families possess with respect to data practices. A few households demonstrate the ability to deploy technical competencies and critical skills in a manner that aligns with Ranjana Das' (2023: 25) category of "alert in practice" families. In this regard, the participating families appear to exhibit varying degrees of data literacy, albeit this literacy is generally low: only some can understand how personal data are generated and processed, and even fewer families can identify or anticipate the social consequences of these processes. Contexts and background resources are important to consider in explaining these variations. Some parents can leverage work skills, abilities, and resources acquired in diverse fields unrelated to technology. Yet, the complexities of data-driven platforms must be taken into account vis-a-vis parental skills since "[u]sing professional competencies...does not necessarily mean that such knowledge applies in all contexts, across all platforms" (Das 2023: 10). While more privacy-oriented families may adopt some protective strategies in one context (e.g., logging-off from Google), most do not care about algorithmically curated feeds and their effects on their child. Consequently, scattered data tactics, such as obfuscation, are often ineffective because they are not motivated by what Pangrazio and Selwyn (2019) identify as "data understanding," let alone "data reflexivity."

Institutional privacy was less considered during the interviews with families, who seem to be somewhat less engaged in reflexivity regarding the implications of the progressive datafication of school, despite it being a field particularly invested by datafication (Jarke and Breiter 2019). Families do not express an awareness of the progressive mediatisation of many aspects of children's routines outside the school, ignoring how they may include broader data collection and use by third parties. These include practices ranging from homework accessed through platforms, to coding courses only available by downloading programs and creating accounts for children, to parent-mediated modes of communication with peers. The analysis cannot disregard the effects of the pandemic as an explanatory factor, which has naturalised many data-based practices in the context of education, creating a great deal of parental fatigue (Aroldi, Zaffaroni, and Cino

2021). In the context of this research, however, the efforts are directed towards identifying potential overlaps between institutional privacy and other privacy contexts. Specifically, parents see teachers as a proxy for privacy relationships in the context of a progressive demand to use connected devices at school. In this respect, more research is needed to understand the privacy implications this might entail.

In conclusion, the results shed light on the dynamic interplay of privacy in everyday life through the conceptual framework of privacy contexts (Livingstone, Stoilova, and Nandagiri 2019). Adopting a threefold framework provides a comprehensive understanding of how privacy-related beliefs and practices are influenced by various contextual factors in participants' lives. By examining the role of temporal and spatial dimensions, social and commercial pressures, and cross-media practices, this paper has contributed valuable theoretical and empirical insights to privacy research.

In this respect, further research could clarify the relationship between contextual dimensions and the factors that support various and sometimes contradictory privacy-related beliefs and practices. A comparative approach would facilitate the analysis of contextual differences and reveal their unexplored connections with potential inequalities—for example, how family groups with varying access to technologies and levels of social integration experience privacy implications due to their social positioning. By doing so, scholars can avoid the risk of "essentializing" the effects of datafication (Mascheroni 2020) and instead capture how privacy concerns evolve in an era of ubiquitous datafication and commercial surveillance, which exerts greater pressure on contemporary parenting.

Acknowledgments

The author is grateful to the two anonymous reviewers for providing important contributions to the manuscript, and to the editors for their significant role in coordinating the publication of this study. With their supportive engagement and thoughtful approach, both proved to be important sources of motivation while improving the article. Furthermore, the author wishes to thank Professor Giovanna Mascheroni for her support throughout the research project and the development of this article.

Funding

The research project DataChildFutures was supported by Fondazione Cariplo – Bando Ricerca Sociale 2019.

References

Ali, Suzan, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef. 2020. Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions. In *Proceedings of the 36th Annual Computer Security Applications Conference, Austin, TX, December 7–11*, 69–83. New York: Association for Computing Machinery.

Amadori, Gaia, and Giovanna Mascheroni. 2024. Situating Data Relations in the Datafied Home: A Methodological Approach. *Big Data & Society* 11 (1): https://doi.org/10.1177/20539517241234268.

Aroldi, Piermarco, Lorenzo Giuseppe Zaffaroni, and Davide Cino. 2021. Il primo lockdown e l'avvio della DAD come banco di prova dei processi di digitalizzazione della scuola italiana, tra disuguaglianze e inclusione. *Sociologia della Comunicazione* 62 (2): 69–86.

Barassi, Veronica. 2020. *Child Data Citizen: How Tech Companies Are Profiling Us from before Birth*. Cambridge, MA: The MIT Press.

Barnes, Renee, and Anna Potter. 2021. Sharenting and arents' Digital Literacy: An Agenda for Future Research. *Communication Research and Practice* 7 (1): 6–20.

Berriman, Liam, and Victoria Jaynes. 2022. Displaying Family in a Digital Age: How Parents Negotiate Technology, Visibility and Privacy. In *Negotiating Families and Personal Lives in the 21st Century*, edited by Sheila Quaid, Catriona Hugman, and Angela Wilcock, 126–139. London: Routledge.

Bietz, Matthew J., Cynthia Cheung, Caryn Kseniya Rubanovich, Cynthia Schairer, and Cinnamon S. Bloss. 2019. Privacy Perceptions and Norms in Youth and Adults. *Clinical Practice in Pediatric Psychology* 7 (1): 93–103.

Blum-Ross, Alicia, and Sonia Livingstone. 2017. "Sharenting," Parent Blogging, and the Boundaries of the Digital Self. *Popular Communication* 15 (2): 110–125.

boyd, danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.

Brown, Barry, Alex S. Taylor, Shahram Izadi, Abigail Sellen, Joseph Jofish' Kaye, and Rachel Eardley. 2007. Locating Family Values: A Field Trial of the Whereabouts Clock. In *UbiComp 2007: Ubiquitous Computing*, edited by John Krumm, Gregory D. Abowd, Aruna Seneviratne, and Thomas Strang, 354–371. Berlin, DE: Springer.

Brunton, Finn, and Helen Nissenbaum. 2016. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: The MIT Press.

Charmaz, Kathy. 2014. *Constructing Grounded Theory*. 2nd edition. London: SAGE.

Chaudron, Stephane, Jackie Marsh, Verònica Donoso Navarette, Wannes Ribbens, Giovanna Mascheroni, David Smahel, Martina Cernikova, Micahel Dreier, Riitta–liisa Korkeamäki, sonia Livinstone, Svenja ottovordemgentschendfelde, Lydia Plowman, Ben Fletcher-Watson, Janice Richardson, Vladimir Shlyapnikov, and Salina Soldatova. 2018. Rules of Engagement: Family Rules on Young Children's Access to and Use of Technologies. In *Digital Childhoods: Technologies and Children's Everyday Lives*, edited by Susan J. Danby, Marilyn Fleer, Christina Davidson, and Maria Hatzigianni, 131–145. New York: Springer.

Couldry, Nick, and Ulises A. Mejias. 2019. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, CA: Stanford University Press.

Damkjaer, Maja Sonne. 2018. Sharenting = Good Parenting? Four Parental Approaches to Sharenting on Facebook. In *Digital Parenting: The Challenges for Families in the Digital Age*, edited by Giovanna Mascheroni, Cristina Ponte, and Ana Jorge, 209–218. Göteborg, SE: Nordicom.

Das, Ranjana. 2023. Contexts and Dimensions of Algorithm Literacies: Parents' Algorithm Literacies amidst the Datafication of Parenthood. *The Communication Review* 27 (1): https://doi.org/10.1080/10714421.2023.2247825.

Das, Ranjana, Niklas Chimirri, Ana Jorge, and Christine Trueltzsch-Wijnen. 2023. Parents' Social Networks, Transitional Moments and the Shaping Role of Digital Communications: An Exploratory Study in Austria, Denmark, England and Portugal. *Families, Relationships and Societies* 1: 1–18.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication* 15 (1): 83–108.

Dencik, Lina. 2018. Surveillance Realism and the Politics of Imagination: Is There No Alternative? *Krisis: Journal for Contemporary Philosophy* 2018 (1): 31–43.

Dias, Patrícia, and Rita Brito. 2020. How Families with Young Children Are Solving the Dilemma between Privacy and Protection by Building Trust—A Portrait from Portugal. *Journal of Children and Media* 14 (1): 56–73.

Hasinoff, Amy Adele. 2017. Where Are You? Location Tracking and the Promise of Child Safety. *Television & New Media* 18 (6): 496–512.

Hodkinson, Paul, and Rachel Brooks. 2023. Caregiving Fathers and the Negotiation of Crossroads: Journeys of Continuity and Change. *The British Journal of Sociology* 74 (1): 35–49.

Isin, Engin, and Evelyn Ruppert. 2015. *Being Digital Citizens*. London: Rowman & Littlefield.

Jarke, Juliane, and Andreas Breiter. 2019. Editorial: The Datafication of Education. *Learning, Media and Technology* 44 (1): 1–6.

Keen, Caroline. 2022. Apathy, Convenience or Irrelevance? Identifying Conceptual Barriers to Safeguarding Children's Data Privacy. *New Media & Society* 24 (1): 50–69.

Kumar, Priya, Shalmali Naik, Utkarsha Devkar, Marshini Chetty, Tamara Clegg, and Jessica Vitak. 2017. "No Telling Passcodes Out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1 (CSCW): https://doi.org/10.1145/3134699.

Leaver, Tama. 2017. Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online. *Social Media + Society* 3 (2): https://doi.org/10.1177/2056305117707192.

Lim, Sun Sun. 2020. *Transcendent Parenting: Raising Children in the Digital Age*. Oxford, UK: Oxford University Press.

Lipu, Merike, and Andra Siibak. 2019. "Take It Down!": Estonian Parents' and Pre-Teens' Opinions and Experiences with Sharenting. *Media International Australia* 170 (1): 57–67.

Livingstone, Sonia, and Alicia Blum-Ross. 2020. *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives*. Oxford, UK: Oxford University Press.

Livingstone, Sonia, and Amanda Third. 2017. Children and Young People's Rights in the Digital Age: An Emerging Agenda. *New Media and Society* 19 (5): 657–670.

Livingstone, Sonia, Mariya Stoilova, and Rishita Nandagiri. 2019. Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review. London: London School of Economics and Political Science.

Lupton, Deborah. 2020. Caring Dataveillance: Women's Use of Apps to Monitor Pregnancy and Children. In *The Routledge Companion to Digital Media and Children*, edited by Lelia Green, Donell Holloway, Kylie Stevenson, Tama Leaver, and Leslie Haddon, 393–402. New York: Routledge.

Lupton, Deborah, and Ben Williamson. 2017. The Datafied Child: The Dataveillance of Children and Implications for Their Rights. *New Media & Society* 19 (5): 780–794.

Lutz, Christoph, and Christian Pieter Hoffmann. 2017. The Dark Side of Online Participation: Exploring Non-, Passive and Negative Participation. *Information, Communication & Society* 20 (6): 876–897.

Lyon, David. 2018. *The Culture of Surveillance: Watching As a Way of Life*. Cambridge, UK: Polity Press.

Mäkinen, Liisa A. 2016. Surveillance On/Off: Examining Home Surveillance Systems from the User's Perspective. *Surveillance & Society* 14 (1): 59–77.

Marwick, Alice E. 2012. The Public Domain: Surveillance in Everyday Life. *Surveillance & Society* 9 (4): 378–393.

Marwick, Alice E., and danah boyd. 2014. Networked Privacy: How Teenagers Negotiate Context in Social Media. *New Media & Society* 16 (7): 1051–1067.

Marx, Gary, and Valerie Steeves. 2010. From the Beginning: Children as Subjects and Agents of Surveillance. *Surveillance & Society* 7 (3/4): 192–230.

Mascheroni, Giovanna. 2014. Parenting the Mobile Internet in Italian Households: Parents' and Children's Discourses. *Journal of Children and Media* 8 (4): 440–456.

———. 2018. Researching Datafied Children as Data Citizens. *Journal of Children and Media* 12 (4): 517–523.

———. 2020. Datafied Childhoods: Contextualising Datafication in Everyday Life. *Current Sociology* 68 (6): 798–813.

———. 2023. The Datafied Habitus: Sociodigital Inequalities and Lived Experiences of Datafication Among Italian Families. Presented at the *The Datafied Family Conference,* University of Surrey, UK, June 28.

Mascheroni, Giovanna, and Kjartan Ólafsson. 2018. Accesso, usi, rischi e opportunità di internet per i ragazzi italiani. I risultati di EU Kids Online 2017. EU Kids Online and OssCom. https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EUKidsOnlineItaly-report-Gennaio-2018.pdf.

Mascheroni, Giovanna, and Andra Siibak. 2021. *Datafied Childhoods: Data Practices and Imaginaries in Children's Lives*. New York: Peter Lang.

Mascheroni, Giovanna, Davide Cino, Gaia Amadori, and Lorenzo Giuseppe Zaffaroni. 2023. (Non-)Sharing as a Form of Maternal Care? The Ambiguous Meanings of Sharenting for Mothers of 0- to-8-Year-Old Children. *Italian Sociological Review* 13 (1): 111–130.

Mehrnezhad, Maryam. 2020. A Cross-Platform Evaluation of Privacy Notices and Tracking Practices. In *2020 IEEE European Symposium on Security and Privacy Workshops, virtual, September 7–11,* 97–106. Genoa, IT: IEEE.

Moser, Carol, Tianying Chen, and Sarita Y. Schoenebeck. 2017. Parents' and Children's Preferences about Parents Sharing about Children on Social Media. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, may 6–11*, 5221–5225. New York,: Association for Computing Machinery.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press.

Pangrazio, Luci, and Neil Selwyn. 2019. "Personal Data Literacies": A Critical Literacies Approach to Enhancing Understandings of Personal Digital Data. *New Media & Society* 21 (2): 419–437.

Plowman, Lydia, and Olivia Stevenson. 2013. Exploring the Quotidian in Young Children's Lives at Home. *Home Cultures* 10: 329–347.

Steijn, Wouter M.P., and Anton Vedder. 2015. Privacy Concerns, Dead or Misunderstood? The Perceptions of Privacy amongst the Young and Old. *Information Polity* 20 (4): 299–311.

Stoilova, Mariya, Rishita Nandagiri, and Sonia Livingstone. 2019. Children's Understanding of Personal Data and Privacy Online—A Systematic Evidence Mapping. *Information, Communication & Society* 24 (4): 557–575.

Sukk, Marit, and Andra Siibak. 2021. Caring Dataveillance and the Construction of "Good Parenting": Estonian Parents' and Pre-Teens' Reflections on the Use of Tracking Technologies. *Communications* 46 (3): 446–467.

Üzümcü, Hamide Elif. 2023. Children's Personal Lives in the Family: Achieving Relational Agency and Individual Privacy in Intrafamilial Relationships in Türkiye. *Children & Society* 38 (4): 1130–1146.

van der Hof, Simone. 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.

van Dijck, Jose. 2014. Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197–208.

Watson, Ash, Deborah Lupton, and Mike Michael. 2023. The Presence and Perceptibility of Personal Digital Data: Findings from a Participant Map Drawing Method. *Visual Studies* 38 (3–4): 594–607.

Zaffaroni, Lorenzo Giuseppe, Gaia Amadori, and Giovanna Mascheroni. 2022. DataChildFutures. Rapporto sui risultati dell'indagine 2020. Zenodo, March 18. https://doi.org/10.5281/zenodo.6367526.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.