Original Manuscript

Childhood
2023, Vol. 0(0) 1–18

DOI: 10.1177/09075682231186486
journals.sagepub.com/home/chd


Children as social actors negotiating their privacy in the digital commercial context

Sonali Srivastava, Terhi-Anna Wilska and Jussi Nyrhinen
Department of Social Sciences and Philosophy, University of Jyvaskyla, Jyvaskyla, Finland

Abstract

This study advances research on children's negotiation of online commercial privacy by identifying an act of digital agency by children that may serve their current needs but can also impact children negatively. Secondly, it identifies certain factors children consider while evaluating the trustworthiness of apps and websites before disclosing information online. Eight focus group discussions with children (13–16 years) in Finland's capital region are analysed using thematic analysis. Our findings highlight that while children's digital literacy education is needed, ensuring that education translates to children's online practices is also essential. We also recommend increasing corporations' accountability in ensuring children's privacy.

Keywords

Children, online privacy, personal data, digital agents, corporate surveillance

Introduction

While participation on various digital platforms provides children with numerous opportunities for education, entertainment, socialising and civic engagement, the opaque data collection practices in digital environments can also expose them to privacy risks and infringe their rights (Milkaite and Lievens, 2019). Ever-evolving tracking technologies like cookies, fingerprint devices and geolocation trackers enable the tracking of users' data in and across various digital platforms in a largely invisible fashion (Turow, 2012; Lupton, 2015). Users' actions in digital environments can now be recorded and converted to data that corporations and governments can use, making data immensely valuable

Corresponding author:
Sonali Srivastava, Department of Social Sciences and Philosophy, University of Jyvaskyla, PO Box 35 FI-40014, Jyvaskyla 40014, Finland.
Email: sonali.s.srivastava@jyu.fi

(Lupton, 2015). The recorded data is mined using algorithms to generate user profiles, and profiling informs the targeted advertising users encounter on digital platforms (Turow, 2012; Lupton, 2015). Large-scale profiling leads to a kind of corporate digital surveillance (Bodle, 2016).

Personal data collection, analysis and subsequent profiling impact children's right to privacy and protection of personal data (UNICEF, 2018). Milkaite and Lievens (2019) point out that children's profiling can be particularly problematic because it can lead to advertisements and content being targeted based on their previous actions online, leading to 'more of the same', thus reducing their exposure to new ideas. UNCRC's articles 13 and 14 that emphasise the right to receive information and freedom of thought, respectively, can be hampered by such profiling (Milkaite and Lievens, 2019). Moreover, such practices can diminish children's and young people's exposure to varied perspectives at a stage in their lives when they explore different identities and make significant life choices (Milkaite and Lievens, 2019). However, children's privacy negotiation practices in the digital commercial context are underexplored (Stoilova et al., 2019). Hence, the present study explores how children aged 13–16 years negotiate their privacy in the digital commercial context. It draws upon childhood studies' conceptualisation of children as social actors (Prout and James, 1990).

It is perhaps more important to explore teenagers' privacy negotiation practices after the General Data Protection Regulation (GDPR) was implemented across the EU in May 2018. This is so because the GDPR's recommendation to fix a digital age of consent between 13–16 years presumes that children in this age cohort are 'able and willing' to manage online consent mechanisms (Keen, 2020: 3). The data of this study consists of eight focus group discussions (FGDs) with 13–16 years old children from schools located in Finland's capital region. This study advances research on children's negotiation of online commercial privacy by exploring the factors that children aged 13–16 years residing in the EU consider while evaluating the trustworthiness of apps and websites before disclosing information online. The study also explores how children exert their agency in the digital commercial context.

This article proceeds as follows: first, we describe how the digital commercial context can undermine children's privacy. We then elaborate on digital agency, followed by a discussion on children's agency in childhood studies. Next, we discuss previous literature on children's privacy negotiation in the digital commercial context before elaborating on the methodology. In the findings, we present how children control the information they disclose online, the practices they adopt for restricting the information they give for commercial profiling, the multiple ways children react to the cookies notification and how children try to manipulate the algorithms to receive their preferred content and advertisements. Our results suggest that when children assess the trustworthiness of apps and websites intuitively, they pay attention to the website's general appearance before disclosing information online. Unlike previous studies, our findings highlight that children are not primarily guided by gut feelings while evaluating the trustworthiness of apps and websites before making online information disclosures. Moreover, the study identifies an act of digital agency by children that may help them exert some influence over the content or advertisements they receive. However, it can also have some negative repercussions on

children. At the end of this article, we discuss the implications of our findings. We conclude by highlighting the limitations and contributions of the study.

Children's privacy and the digital commercial context

Sonia Livingstone and colleagues (2019a:13) identify three contexts or relationships in digital environments where users' privacy matters: 'between an individual and (i) other individuals or groups (interpersonal privacy); (ii) a public sector or third sector (institutional privacy); or (iii) a commercial for-profit organisation (commercial privacy).' Commercial privacy is defined as 'how my personal data is harvested and used for business and marketing purposes' (Livingstone et al., 2019b: 4). To distinguish the different kinds of data that circulate in digital environments, Simone van der Hof (2016) divides data into three types. First, 'data shared' includes data shared by users knowingly but not necessarily intentionally, such as content posted on social media platforms and personal information given while registering on apps or websites. Second, 'data given off' or behavioural data consists of data left mostly unknowingly by users through their online activities. It includes search history, clicks, likes, device location, videos watched, time spent browsing a page, etcetera. Cookies and other tracking technologies track data given off. Finally, 'inferred data' (also called profiling) is derived from analysing 'data shared', 'data given off' and possibly data from other sources, usually by employing algorithms. In this study, we use van der Hof's (2016) data typology and focus on the digital commercial context and therefore commercial privacy. 'Inferred data' that forms the basis of targeted adverting is the most pertinent in the commercial context (Stoilova et al., 2020).

Exercising control over data collection for commercial purposes on digital platforms is challenging for users because such data collection takes place in a largely invisible fashion (Montgomery, 2015). Actions and interactions that previously went unrecorded can now be recorded in digital environments, making privacy something that always needs to be negotiated instead of being a given (Livingstone et al., 2019a). Children share a one-way relationship with marketers who collect their data online, and this leaves little scope for the negotiation of privacy (Steeves and Reagan, 2014). Consent is used to legitimise the act of watching over data subjects (van der Hof, 2016) but they have no options to revoke this consent (Steeves and Reagan, 2014). Moreover, the complex language of privacy policies makes it difficult for users to understand what they consent to, rendering the notice-and-consent model ineffective in addressing the asymmetrical power relationship between users and data collectors (Waldman, 2018).

Waldman (2018) notes that users' online information disclosure and consent decisions are often based on factors like trust and proposes that trust should be the benchmark of privacy legislation. Once users entrust corporations with their data, the latter should act as 'fiduciaries' of users' information (Waldman, 2018:87). As 'information fiduciaries', companies should ensure that they do not misuse this data to manipulate users, and privacy legislation must ensure that companies do not abuse users' trust (Waldman, 2018: 88).

Users' digital agency

Within the all-encompassing structures of digital surveillance, some scholars have called upon users to exert their digital agency (for example, Beer, 2009; Kennedy and Moss, 2015). Better knowledge of online personal data collection and mining processes and how they determine users' digital experiences and choices is one way to develop users' digital agency (Beer, 2009). Beer (2009) envisages that through such knowledge, users can determine the information they share and steer the algorithms in the direction they wish them to take. This could lead to skilled agents acting in reflexive ways instead of fully resisting the algorithms (Beer, 2009). Kennedy and Moss (2015) opine that digital agency can be promoted if 'publics' begin to determine how they are represented instead of vice versa.

When it comes to children's agency, childhood studies scholars Allison James and Alan Prout (1990) emphasise the importance of recognising children as social actors, agentic in shaping their social lives and that of others around them. The central idea was to give a voice to children and challenge the dominant view of children as incomplete 'becomings' (Oswell, 2013: 40). However, scholars from within the field have critically engaged with the idea of children's agency (for example, Oswell, 2013; Spyrou, 2018). One point of critical reflection has been the tendency to view children's agency as essentially positive. Such a view could disregard that children may not necessarily act in their or others' best interests while being agentic (Valentine, 2011; Spyrou, 2018). Abebe (2019) invites childhood studies researchers not just to recognise the existence of children's agency but to consider what kind of agency it is and what purpose it serves.

Previous research on children's negotiation of online commercial privacy

Studies on children's strategies to navigate online privacy have focussed mainly on data given knowingly (Stoilova et al., 2019). In relation to the latter, Marwick et al. (2010) observe that privacy protection strategies of adolescents fall under the categories of avoidance and approach. Avoidance strategies include refraining from using certain websites, and approach strategies involve taking active steps to protect privacy like providing false information and reading privacy statements (Youn, 2009). Previous studies on teenagers' privacy protection practices report that they often share incomplete personal information with websites (Youn, 2005; Lenhart et al., 2011) and rarely read privacy statements on them (Youn, 2005).

Few studies have explored children's online privacy negotiation practices in the digital commercial context (Stoilova et al., 2019). In Pangrazio and Selwyn's (2018) workshop, organised before developing an app to support children's privacy management practices, a few participants (aged 11–17 years) reported using a VPN to protect personal data. Their participants found online privacy notifications lengthy and complicated to read (Pangrazio and Selwyn, 2018). Stoilova et al. (2020) note that incomprehensible privacy terms on websites and difficult to disable cookies lead children to experience a sense of powerlessness against personal data collection for commercial purposes. Many

participants in their study carried a misconception that strategies like providing a fake name and age, which they used in the interpersonal context, can also protect them from commercial actors (Stoilova et al., 2020). Holvoet et al. (2021) found that trust played a significant role in children's (aged 12–14 years) online consent decisions. Some of their participants trusted big companies' websites or checked if the website was secure before accepting cookies. In their study, children usually accepted cookies without reading the terms, and some did so to move ahead with their online activities. Holvoet et al. (2021) note that trust also played an important role in children's online information disclosure decisions. They report that while evaluating the trustworthiness of apps and websites, children were guided mainly by a gut feeling. A few participants, though, could 'recognise signals referring to suspicious data requests' (Holvoet et al., 2021:322), which suggests that upon receiving data requests on a website or app, some participants could recognise certain requests as suspicious. However, Holvoet et al. (2021) do not adequately clarify what their participants considered or paid attention to when they were guided by their gut feelings while evaluating the trustworthiness of websites and apps.

The present study contributes to the existing literature on children's negotiation of privacy in the digital commercial context by providing insights into how children residing in the EU evaluate the trustworthiness of apps and websites before making online information disclosure decisions and how they exert their agency in the digital commercial context. The study poses the following research question:

RQ – How do children aged 13–16 years negotiate their privacy in the digital commercial context?

Methodology

This article uses data from eight FGDs conducted in schools across Finland's capital area to explore children's understanding and negotiation of privacy in the digital commercial context and their perspectives on targeted advertising. The digital age of consent in Finland is 13 years, and the GDPR recommends that EU member states fix this age between 13–16 years (Livingstone, 2018). Therefore, children aged 13–16 years were recruited for the study. FGDs are helpful in gathering children's perspectives through a dialogical process (Gibson, 2012). They simulate a peer group situation which can facilitate the participation of children who may not want to speak individually with adults in interviews (Horner, 2000). Small group sizes of 4–6 children are optimal as they replicate common peer group interactions (Eder and Fingerson, 2002). Hence, each group consisted of 4–6 participants. Table 1 summarises the group composition. All the 38 participants were recruited by their schools. Eight FGDs were conducted, out of which five were in Finnish. Three FGDs were conducted in English because the school was bilingual (English and Finnish). Students attending bilingual schools often belong to different nationalities. The average length of an FGD was 50 min. The data collection took place between December 2020 and May 2021.

According to the guidelines for the responsible conduct of research in Finland, we gathered informed consent from participants aged 15 years and above and from their parents in the case of participants below 15 years (TENK, 2019). We tried to ensure a clear

Table 1. Summary of group composition.

Group	School	Boys	Girls	Age (Years)
1	Bilingual	1	4	13–14
2	Bilingual	2	3	14–15
3	Bilingual	2	2	15–16
4	Finnish	0	4	15–16
5	Finnish	3	1	15–16
6	Finnish	2	3	15–16
7	Finnish	2	3	14–15
8	Finnish	2	4	15–16

understanding of informed consent by repeating the consent terms and inviting questions before the FGDs. The voluntary nature of consent was reiterated. One group informed that they had recently attended a school lesson on privacy protection. Hence, they could have better privacy negotiation practices. We will refer to this group as Focus Group Lesson (FGL henceforth) to distinguish the responses of its participants. The rest of the groups will be denoted as Focus Group Standard (FGS henceforth).

Christensen and Prout (2002) recommend adopting the 'ethical symmetry' approach between children and adults in research that views children as social actors. This mainly involves not treating children as unequal or inferior to adults. However, they caution that researchers should not ignore the power imbalance between children and adults arising from generational differences. We were mindful of this power imbalance and tried to bridge it by interacting with the participants in a friendly manner. We also showed our inclination to learn from them and asked them to give us tips to protect our personal data, just as we would ask adult participants. The school environment can exacerbate children's feelings of being evaluated, and adult researchers must stress that there are no right or wrong answers (Punch, 2002). We emphasised the latter and highlighted that there were multiple perspectives based on experiences. Moreover, we often reiterated that even we get confused with various online notifications.

Differences between children, like varied articulation abilities, extroversion and introversion, should not be ignored (Punch, 2002). We tried to facilitate equal participation by keeping in mind the differences between children. Firstly, simple points like taking turns to speak and re-asking the moderator if something is unclear (Gibson, 2012) were highlighted before the FGDs. Moreover, two researchers were always present in the FGDs, and one of us acted as an observer. Since attending to non-verbal cues can support quiet participants (Sim, 1998), the observer was assigned this task. To avoid domination of older children over younger ones (Gibson, 2007), we requested that the teachers organise groups with children from the same grade. Small group sizes were also conducive to equal participation.

Using van der Hof's (2016) data typology, we showed our participants screenshots of scenarios where data is given (registering options on an app and website), given away (a webpage with cookies notification) and images of targeted advertisements based on

inferred data. Cookies are files installed by a website on the browser, so accepting cookies enables tracking of users' online activities (Rafter, 2022) or data 'given away'. Our discussions centred around using various apps and websites and browsing the internet on different devices. Since content shared on social media platforms also constitutes data given (van der Hof, 2016), we tried to gauge whether our participants contemplated controlling the content they shared. We did not want to use the word privacy as that could influence participants' responses. Hence, we used indirect probes like asking why they visited their favourite social media platforms, and in some groups the participants themselves discussed this. Since starting the discussion with something simple and familiar helps build engagement and informality (Gibson, 2012), we asked the participants to name their favourite app while introducing themselves. Similarly, the screenshots that we showed them were from social networks like Instagram and TikTok and gaming apps like Fortnite that are popular among this age cohort.

The audio recorded FGDs were transcribed and anonymised. Transcriptions in Finnish were translated into English. The data was analysed using thematic analysis (Braun and Clarke, 2006).

Children's negotiation of privacy in the digital commercial context

Controlling information shared knowingly

Stoilova et al. (2020) note that many participants in their study thought that strategies used to protect interpersonal privacy like using fake name and age would also help them protect their privacy against commercial actors. Similarly, when we discussed how the participants shared their personal information while registering on apps and websites, most children reported faking their age. However, for all the groups, the motivation for faking age was not related to protecting personal information but to getting permission to use apps with a higher age limit.

> 'Yeah, because not all apps let you in if you are under 16 or at least under 13. So, you won't get in anywhere.' (Jutta, 15)

Children assess the trustworthiness of apps and websites before disclosing information (Holvoet et al., 2021). Similarly, many children, but none from FGL, discussed how suspicious apps or websites raised a red flag for them. While evaluating the trustworthiness of apps and websites, children are primarily guided by gut feelings (Holvoet et al., 2021). A few participants in our study were also somewhat guided by intuition. They mentioned looking at a website's layout or appearance to identify an untrustworthy website.

> 'I feel like there's really rarely you do come across a site where if you are looking for information on something and it asks you to sign in but looks … just the layout of the site is bad and when you press something it goes somewhere else and weird stuff like that, then I would leave the app and go and find something more trustworthy.' (Tapio, 15)

However, some children also reported looking for concrete signs to identify suspicious websites or apps before sharing their information. Olli (15) considered a missing lock symbol as a sign of concern: 'well I don't know, […].usually, there always is a lock if it's safe, there up.[…]' Nick (15) reported withholding his information on a site with lots of pop-up ads: 'or I tend not to put my information if there are a lot of those pop-up ads.'

A few children reported not relying solely on their assessments. Instead, they searched for more information before making information disclosures.

> ' […] And umm but before I do that (provide my email) I usually check or sometimes I search on the internet like is this website trustable and like that it's not a scam or something like that.' (Tiina, 13).

An avoidance strategy (Marwick et al., 2010) was also reported by some participants from FGS who avoided registering on websites that they would use infrequently.

> 'If I like use it often, then I might make an account, but if it's just random, I won't.' (Rita, 14)

Despite the care the participants exercised before registering on websites, registering options per se were not viewed suspiciously. Registering on websites using Google and Facebook can expose users' personal data to various websites (Stokes, 2017). When asked what they chose when given an alternative between registering through these options or creating their account, most participants reported using Google or Facebook. Only one participant from FGS mentioned not choosing either because of her mother's warnings.

> 'My mum told me that I shouldn't, and I think I read an article about it too.' (Suvi,15)

Many participants reported watching content on YouTube, TikTok and Instagram instead of actively posting there, but it was challenging to ascertain if this was due to privacy concerns or other reasons like shyness. However, the persistence and searchability of data on social media platforms (boyd and Marwick, 2011) was a cause of concern for a few participants from FGS who reported considering their sharing practices on apps.

> Tiina (13): Yeah, if you like accept the cookies, it, for example, says that *TikTok* is allowed your data. And like the videos you post, even if you have a private account and then you accept it, then they like get the data. They like said in the privacy policy, and most of the people don't read it through. So they'll usually like accept it without seeing like what they are accepting.
>
> Rahul (13): Yeah, I just wanted to add that my dad says that 'if you put something on the internet, it never comes out of there and stays there.'

Inferred data that forms the basis of targeted advertising consists of 'data given' and 'data given off' (van der Hof, 2016). Therefore, by adopting these practices, children made some attempts at privacy protection that would also have some protective impact on

their privacy against commercial actors. It is important to point out that we found it challenging to understand if the motivation to share personal information cautiously was with commercial operators in mind or for general e-safety. Multiple actors seemed to be on children's minds when they reported controlling the information shared knowingly in digital environments. They used the word 'they' to describe those who could access and use their data. When probed further about who they thought these 'they' were, the participants came up with various answers like 'the marketers', 'people who make these websites', 'the app'. Nevertheless, the practices reported by our participants reflect a general caution they exercise in digital environments.

Controlling the information given specifically for commercial profiling

The data sharing mechanisms that our participants mentioned above were with multiple actors in mind. Therefore, we talked about the practices they adopted to control the information given to apps and websites that could potentially be used for commercial profiling. We did this by showing our participants screenshots of targeted advertisements on Instagram and product suggestions during web surfing and asking them if they had ever tried to make these advertisements incongruent with their preferences or reduce or control the information they give to the internet.

Diana (15, FGL) explained a mechanism of control like deleting search history:

> 'I also have this thing in *Google* that it does not save my search history. It's turned off completely. It's like I can't even see what I have searched because it's not there.'

Some participants from FGL talked about using 'private mode', although they were unsure if it protects all the data:

> Interviewer: Have you ever tried to reduce or control the amount of information you give?
>
> Lasse (14): At least I have put the setting in Google so that it doesn't collect the information.
>
> Ari (14): Private mode
>
> Interviewer: What? Private mode?
>
> Fiia (15): So, it goes to a private browser and doesn't collect the information.
>
> Lasse: Remember.
>
> Fiia: I don't know if it allows cookies.

Jutta (15) from FGS mentioned occasionally controlling the access of websites to her phone memory:

> 'I may have occasionally tried not to give all the permissions right away. I have thought for a moment if I have to give all the permissions to websites to the files on my computer or on my phone. When you download an application, they ask for access to the memory of the phone,

and you consider if you can use that application without giving your permission. And with that, I try to limit it a bit.'

Like in Pangrazio and Selwyn's (2018) study, a few participants from FGS in our study also reported using a VPN sometimes. Rahul (13), reported occasionally using a VPN: 'Maybe if you use VPN, they can't really track you because everything that you have is not actually you.'

Very few participants adopted the data protection practices mentioned above. The children who did so belonged to both FGL and FGS.

Multiple ways of using cookies notification

The EU cookies directive makes it mandatory to notify users in the EU about the presence of cookies on apps and websites, apprise them about how the data collected using cookies will be used and give them the option to accept or refuse the use of cookies (Ansari, 2022). This directive also applies to those cookies that track users' location data (Slack, 2022). We showed our participants a screenshot of a cookie notification with the options 'accept all' and 'cookies settings'. They mentioned noticing the same or similar notifications on various websites. We then asked our participants how they usually reacted to such notifications. Most children accept cookies without reading the terms (Holvoet et al., 2021). Somewhat similarly, some of our participants reported accepting cookies unthinkingly.

'I don't know. I haven't ever thought about it. I always just accept them.' (Kaisu,16).

Children often accept cookies to get a faster passage to the app or website (Holvoet et al., 2021). Likewise, some of our participants, including a few from FGL, accepted cookies to quickly move on with their online activities.

'Well, usually I accept all the cookies because that is how I can quickly go to browse what I want to.' (Rhea, 15)

Children find it challenging to manage their privacy by reading lengthy terms and conditions of consent (Pangrazio and Selwyn, 2018). Similarly, many participants, including some from FGL, got discouraged by the difficult language and exhaustive terms when they tried to modify privacy notifications.

'Yeah, I feel like it's very hard to understand. And there's like a lot of things and that it's just a lot easier to press "accept all cookies".' (Rita, 14)

A few participants, including some from FGL, reported hiding location data. Tom (15) noted: '[…]. I sometimes remove the location information if I can.'

Trust plays a vital role in children's online consent decisions (Holvoet et al., 2021). Similarly, some children from FGS, but none from FGL, mentioned assessing the

trustworthiness of websites before accepting cookies. Kia (16) said: 'I check the overall site, where I am, and is it reliable at all […]. I don't maybe accept straight away.'

They evaluated trustworthiness based on various factors. Children often trust big companies and accept cookies on their websites (Holvoet et al., 2021). Likewise, some participants from FGS trusted big companies' websites.

> 'If it's a known website or belongs to a big company, I usually put "I accept".' (Paul,15)

Sites without a secure symbol were not trusted (Holvoet et al., 2021). Similarly, a few participants from FGS reported not accepting cookies where the secure symbol was missing

> 'More often I see whether it is sketchy or not when at the top it says, "not secure".' (Lucia, 13)

Participants in one FGS, where some children reported not accepting cookies on suspicious sites, described the signs they looked for to identify untrustworthy websites. Kim (15) mentioned paying attention to the language: 'If you can clearly see that they have been translated with *Google Translate*, and they just look suspicious.' Tom (15) recommended studying the domain name: '[…] if the website's name is just a mixture of numbers and letters, it's shady.'

Discussions at school shape privacy concerns (Stoilova et al., 2020). Similarly, some, but not all, participants from FGL reported checking cookies and accepting only mandatory ones whenever possible.

> 'Before, I always did so that I just accepted straight away, but after when we talked about this in one of our Finnish lessons, I have started to look through them a little or like see if I can only accept the mandatory ones, then I choose that option or sometimes I just block them all.' (Satu, 14, FGL)

A few participants from FGS also mentioned selecting only the mandatory cookies.

> 'Yes, I also have almost the same. If you see there is still the option that says the minimum cookies, then I press it.' (Sam,15)

Tactic reflecting a paradoxical view of control

Until now, the practices discussed are broadly based on an interpretation of control as taking steps to withhold information. However, participants in two groups also discussed a tactic that overturned this idea of control. A somewhat paradoxical view of control underpins the tactic that we report now.

When asked if there is any way to stop the ads from being highly accurate about them or the internet from knowing what they like, the participants in one FGS mentioned pre-selecting the content that interested them. They reported doing so to avoid irrelevant content and advertisements. Olli (15) said: 'but in some apps, you can select by yourself

what you are interested in. For example, on *Pinterest* and those like *Spotify*, you can select what music you like, and these kinds of things will come.' Kaisu (16) chimed in, 'Yeah, I have, on *Pinterest*.'

In FGL, one participant mentioned searching and deliberately 'liking' posts about the things she wanted.

> Interviewer: okay, do you guys think that there is any way to control ads or stop them from being too accurate about you? Or stop the internet from knowing what you are doing? Do you have any advise?
>
> Fiia (15, FGL): I remember at least once when I wanted pictures of a certain thing […] so I started to type and search for it and liked some posts so that it (app/website) would know that I want them.
>
> Interviewer: So, you went to do it on purpose?
>
> Fiia: Yes

Two more participants joined in this conversation and reported managing their 'likes' and scrolling pace to receive what interested them. They responded to a question related to advertisements. However, we are unsure if the participants' use of the term 'videos' means video advertisements, content videos, or both because both appear on Instagram and TikTok. Either way, they give information about their preferences.

> Satu (14, FGL): I have done so in *TikTok* that when there started coming a lot of things that I didn't like at all, then I started liking more videos (advertisements and/or content) that interested me so I would get more of those (videos).
>
> Diana (15, FGL): I have noticed on *Instagram* and *TikTok* that when you stop at something while scrolling then you get more of those (content and/or advertisements). So, like if there's something I don't like, then I just go past it very quickly so that it (*Instagram or TikTok*) would know that I don't like them. […].

A rather simplistic way to interpret these children's paradoxical view of control is that they provide more accurate information about themselves for commercial profiling and thus compromise their privacy. However, considering that users' digital agency can involve steering the algorithms to suit themselves (Beer, 2009), such a tactic could also be viewed as an exercise of digital agency. These participants understand that their actions leave traces in digital environments. Based on this knowledge, they try to modulate their actions to influence the content or advertisements they receive. By doing so, they also give more precise information for their commercial profiling. While this does not protect these children's privacy, this could also be viewed as an attempt to utilise online profiling to receive what they find relevant or useful. Children in other groups mentioned either scrolling past irrelevant advertisements or enjoying relevant advertisements when they received them. However, none of the other groups reported trying to influence the content or advertisements they received, as these two groups did.

Discussion

In this study, we explored how children negotiate their privacy in the digital commercial context. Our thematic analysis of eight FGDs ($n = 38$) with children aged 13–16 years in Finland suggests that children adopted the following practices: (i) controlling information shared knowingly, (ii) controlling the information given specifically for commercial profiling, (iii) multiple ways of using cookies notification and (iv) a tactic reflecting a paradoxical view of control.

Controlling information shared knowingly reflects that many children, but none from FGL, made online information disclosure decisions based on trust. Here our findings concur with Holvoet et al.'s (2021) research. Holvoet et al. (2021) found that while evaluating the trustworthiness of apps and websites, children were primarily guided by gut feelings. However, their research does not elaborate on what kind of factors their participants paid attention to when they used their gut feelings to evaluate websites. We found that when children evaluated apps and websites intuitively, they paid attention to the general appearance or layout of the website before making information disclosures. To the best of our knowledge, previous studies have not noted this. Unlike Holvoet et al.'s (2021) study, our participants were not primarily guided by gut feelings while evaluating the trustworthiness of apps and websites. Although some children evaluated websites intuitively, others mentioned looking for specific signs of suspicion on websites and apps and reported withholding information when they noticed such signs. A few of our participants even reported searching for information about websites before making information disclosures. Additionally, we found that registering options raised privacy concerns for only one child from FGS, which reflects the need to improve children's awareness of online data flows. Only a few children from FGL and FGS reported restricting the information given specifically for commercial profiling. This indicates that more efforts are required to improve children's awareness of data protection mechanisms.

Multiple ways of using cookies notification reflect children's varied ways of reacting to cookies notification. We found that some children accepted cookies either unthinkingly or to move ahead with their online activities. This reflects the need to build more awareness about editing privacy notifications to control online tracking. Many children, including some from FGL, reported getting discouraged by the incomprehensible language of privacy notifications when they tried to modify them. This indicates that difficult to edit cookies can lead children to experience powerlessness against digital data collection (Stoilova et al., 2020). Like in Holvoet et al.'s (2021) study, in our research as well some children, but none from FGL, based their consent decisions on trust and accepted cookies on big companies' websites. The latter reflects children's misconceptions and raises the need to educate children about varied types of cookies because even big companies' websites can use third-party cookies. Like Holvoet et al. (2021), we also found that some children from FGS refrained from accepting cookies on unsecure websites. Additionally, we found that children from FGS looked for various signs to evaluate the trustworthiness of websites before accepting cookies, which reflects their general caution in online environments. A few children accepted mandatory cookies whenever possible, and this

has not been observed in previous studies. The children who did so belonged to both FGL and FGS. It suggests that implementing their knowledge of privacy management mechanisms helps children in protecting their personal data.

To the best of our knowledge, the tactic reflecting a paradoxical view of control has not been observed in previous studies. It is both agentic and problematic. The children who adopted this tactic provided information for more precise profiling. However, they also tried to exert some control over what gets done with their data. These children did not resist the algorithms but acted as reflexive agents who guided the algorithms in the direction the children desired (Beer, 2009). Childhood studies scholars caution that children's agency might not necessarily have positive implications (Valentine, 2011; Spyrou, 2018). It is essential to consider what purpose children's agency serves (Abebe, 2019). Therefore, it is vital to examine what implications this act of digital agency may have for children. While children might experience a sense of control by receiving relevant content or advertisements, eventually, it is the marketers who benefit from children's act of digital agency because they receive more accurate information for profiling children. Through their agentic actions, the children ensure the effectiveness of algorithms, thus augmenting corporate digital surveillance.

This act of digital agency can be particularly problematic for children for two main reasons. Firstly, from a children's rights perspective, practices like profiling and targeting, where children receive content and advertisements based on their previous online actions, hinder children's right to receive information and freedom of thought because they keep receiving content that matches their preferences, thus reducing their exposure to new ideas (Milkaite and Lievens, 2019). Secondly, such practices can be concerning as they may reduce children's and young people's access to multiple viewpoints at a life stage when they explore various identities and make important life choices (Milkaite and Lievens, 2019). Therefore, by disclosing data about their preferences and aiding the accuracy of algorithms, these children themselves reduce their exposure to new ideas and choices, which can have various negative ramifications.

Children's privacy against commercial actors is an important policy concern (Livingstone et al., 2019a). Hence, our results have broader implications. Researchers have called upon corporations to play a more significant role in ensuring that children's online privacy rights are protected (Stoilova et al., 2020; Pangrazio and Selwyn, 2018). Based on our findings, we support this view. Firstly, given that children found it hard to comprehend and edit lengthy privacy terms, we support previous researchers who have urged corporations to simplify privacy notifications (Stoilova et al., 2020; Pangrazio and Selwyn, 2018). Secondly, our finding that trust plays a pivotal role in children's privacy management decisions raises the need to increase corporations' accountability. Therefore, we endorse Waldman's (2018:88) recommendation that once users entrust corporations with their data, corporations should act as 'information fiduciaries', and privacy legislation must ensure that corporations uphold the trust that users posit in them. Waldman's (2018) proposal could help in increasing corporations' accountability in ensuring that children's online data is protected.

We observed that children from FGL and FGS adopted almost similar privacy negotiation practices. Moreover, it was concerning that the tactic with a paradoxical view of control, which made children vulnerable to more accurate profiling, was primarily adopted by children from FGL. We support the calls for increasing children's digital literacy (Stoilova et al., 2020; Pangrazio and Selwyn, 2018), especially their knowledge of cookies. However, our findings also suggest that it is crucial to ensure that privacy education translates to children's everyday practices and actions.

Conclusion

Like all studies, this study suffers from certain limitations. Bühler-Niederberger (2010: 379) underscores that research with children must consider the 'horizontal dimension' of differences between children that can limit their possibilities to act. Children's digital competencies can greatly differ due to factors including their socio-economic background and technical skills (Livingstone et al., 2019a). This study does not take into consideration children from different socio-economic backgrounds or from certain school districts. Moreover, it only considers schools in an urban setting like the capital area of Finland.

Despite the limitations enumerated above, this study makes some important contributions. It identifies an act of digital agency by children that may help children exert some influence over the content and advertisements they receive. However, it can also have various negative implications for children as it enhances the commercial digital surveillance of children and may reduce their access to new choices and viewpoints. Secondly, our research highlights that when children evaluate the trustworthiness of apps and websites intuitively, they pay attention to the appearance of a website. Moreover, unlike previous research, this study highlights that children are not primarily guided by gut feelings while evaluating the trustworthiness of apps and websites before disclosing information online. Although some children assessed websites intuitively, others identified specific signs of suspicion. A few children even searched for information about websites before making information disclosures.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This study is funded by the Strategic Research Council at the Academy of Finland, grant #327237 and the Academy of Finland, grant #320370.

ORCID iD

Sonali Srivastava https://orcid.org/0000-0003-1871-5023

References

Abebe T (2019) Reconceptualising children's agency as continuum and interdependence. *Social Sciences* 8(3): 81.

Ansari M (2022) Eu cookies directive. In: *FreePrivacyPolicy*. Available at https://www.freeprivacypolicy.com/blog/eu-cookies-directive/#2_Have_A_Cookies_Policy (Accessed 25 April 2023).

Braun V and Clarke V (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology* 3(77): 77–101.

Beer D (2009) Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media and Society* 11(6): 985–1002. DOI: 10.1177/1461444809336551.

Bodle R (2016) A critical theory of advertising as surveillance. In: Hamilton J, Bodle R and Korin E (eds) *Explorations in Critical Studies of Advertising*. Abingdon: Routledge, pp. 138–152.

boyd D and Marwick AE (2011) Social privacy in networked publics: teens' attitudes, practices, and strategies. In: *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. Oxford, UK: pp. 1–29.

Bühler-Niederberger D (2010) Childhood sociology in ten countries: current outcomes and future directions. *Current Sociology* 58(2): 369–384.

Christensen P and Prout A (2002) Working with ethical symmetry in social research with children. *Childhood* 9(4): 477–497. DOI: 10.1177/0907568202009004007.

Eder D and Fingerson L (2002) Interviewing children and adolescents. In: Gubrium JF and Holstein JA (eds) *Handbook of Interview Research: Context and Method*. Thousand Oaks: Sage, pp. 181–201.

Finnish National Board on Research Integrity (TENK) guidelines (2019) The ethical principles of research with human participants and ethical review in the human sciences in Finland. Available at https://www.tenk.fi/sites/tenk.fi/files/Ihmistieteiden_eettisen_ennakkoarvioinnin_ohje_2019.pdf.

Gibson F (2007) Conducting focus groups with children and young people: strategies for success. *Journal of Research in Nursing* 12: 473–483.

Gibson F (2012) Interviews and focus groups with children: methods that match children's developing competencies. *Journal of Family Theory and Review* 4: 148–159. DOI: 10.1111/j.1756-2589.2012.00119.x.

Holvoet S, Jans SD, Wolfg RD, et al. (2021) Exploring teenagers' folk theories and coping strategies regarding commercial data collection and personalized advertising. *Media and Communication* 10(1): 317–328.

Horner SD (2000) Using focus group methods with middle school children. *Research in Nursing and Health* 23(6): 510–517.

James A and Prout A (1990) *Constructing and Reconstructing Childhood: Contemporary Issues in the Sociological Study of Childhood*. London: Falmer Press.

Keen C (2020) Apathy, convenience or irrelevance? Identifying conceptual barriers to safeguarding children's data privacy. *New Media and Society* 24: 50–69.

Kennedy H and Moss G (2015) Known or knowing publics? Social media data mining and the question of public agency. *Big Data and Society* 2(2): 1–11. DOI: 10.1177/2053951715611145.

Livingstone S (2018) Children: a special case for privacy? *Intermedia* 46(2): 18–23.

Livingstone S, Stoilova M and Nandagiri R (2019a) *Children's Data and Privacy Online: Growing up in a Digital Age: An Evidence Review*. London: London School of Economics and Political Science.

Livingstone S, Stoilova M and Nandagiri R (2019b) *Talking to Children about Data and Privacy Online: Research Methodology*. London: London School of Economics and Political Science.

Lenhart A, Madden M, Smith A, et al. (2011) Teens, kindness and cruelty on social network sites: how American teens navigate the new world of 'digital citizenship. Report. Available at http://www.pewinternet.org/~/media/Files/Reports/2011/PIP_Teens_Kindness_Cruelty_SNS_Report_Nov_2011_FINAL_110711.pdf.

Lupton D (2015) *Digital Sociology*. Abingdon: Routledge.

Marwick AE, Murgia-Diaz D and Palfrey JG (2010) Youth, privacy and reputation (literature review). http://papers. ssrn.com/sol3/papers.cfm?abstract_id=1588163.

Milkaite I and Lievens E (2019) Children's rights to privacy and data protection around the world: challenges in the digital Realm. *European Journal of Law and Technology* 10(1).

Montgomery KC (2015) Youth and surveillance in the facebook era: policy interventions and social implications. *Telecommunications Policy* 39: 771–786.

Oswell D (2013) *The Agency of Children. From Family to Global Human Rights*. Cambridge: Cambridge University Press.

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

Punch S (2002) Research with children: the same or different from research with adults? *Childhood* 9(3): 321–341.

Rafter D (2022) What are cookies? In NortonLifeLock. Available at: https://us.norton.com/blog/how-to/what-are-cookies (Accessed 20 January 2023).

Sim J (1998) Collecting and analysing qualitative data: issues raised by the focus group. *Journal of Advanced Nursing* 28: 345–352.

Slack C (2022) Privacy practices for user location. In: *FreePrivacyPolicy*. Available at https://www.freeprivacypolicy.com/blog/user-location-privacy-practices/ (Accessed 25 April 2023).

Spyrou S (2018) What kind of agency for children? In: Spyrou S (ed) *Disclosing Childhoods*. London: Palgrave Macmillan, pp. 117–156.

Steeves V and 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, Livingstone S and Nandagiri R (2019) Children's understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication and Society* 24. DOI: 10.1080/1369118X.2019.1657164.

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

Stokes N (2017) Should you use facebook or google to log in to other sites? In: *Techlicious*. Available at https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/ (Accessed 25 November 2021).

Turow J (2012) *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven: Yale University Press.

UNICEF (2018) *Children's Online Privacy and Freedom of Expression*. New York, NY: UNICEF.

Valentine K (2011) Accounting for agency. *Children and Society* 25(5): 347–358.

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.

Waldman AE (2018) *Privacy as Trust: Information Privacy for an Information Age*. Cambridge: Cambridge University Press.

Youn S (2005) teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting and Electronic Media* 49(1): 86–110.

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