COGITATIO

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

Article

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

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

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

* Corresponding author

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

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

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

Issue
This article is part of the issue "Children's Voices on Privacy Management and Data Responsibilization" edited by Ralf De Wolf (Ghent University, Belgium) and Mariek Vanden Abeele (Tilburg University, The Netherlands).

1. Introduction

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

Parents have thus been given a crucial legal responsibility in their children's online data management, and can fulfil this role by, for instance, applying safety measures. One study, for instance, found that children who had indicated that their parents impose certain restrictions on what they could watch on YouTube, had better online safety beliefs (e.g., the degree to which they, for instance, believed that their online data goes away when leaving the internet (Andrews, Walker, & Kees, 2020). Despite this important parental role, academic research has rarely examined parents' view on online

commercial data collection practices, and whether and how they take up this responsibility. The limited research on general privacy issues suggests that parents are concerned about the information collected from their kids (Anderson, 2019), yet often feel unsure about addressing general online safety issues (Third, Spry, & Locke, 2013). A lack of data protection knowledge is, however, commonly associated with the inability to effectively regulate one's online privacy (Trepte et al., 2015). This may thus imply that parents are potentially unable to optimally manage their own online privacy, which subsequently questions their ability to take on a role as caretaker of their children's online privacy. In this perspective, it might also be interesting to explore whether children themselves have insights on how they can manage their own online privacy. Although previous studies (Park, 2013; Park, Campbell, & Kwak, 2012; Youn, 2009) showed that people can engage in a range of privacy protective measures which they deem appropriate to safeguard their privacy and data (e.g., closing the website, giving fake data), little research actually explored how children and parents use these strategies to cope with online data requests from commercial entities.

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

2. Related Work

2.1. Different Types of Commercial Data Collection

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

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

2.2. Strategies to Cope with Data Collection

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

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

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

2.3. Children's Privacy Perceptions

When it comes to children, we assume perceptions of privacy and personal data is subject to age due to developmental and cognitive differences. The developmental process through which children go is related to their cognitive maturation and entails acquiring various skills concerning cognitive resources and theory of mind, or the recognition that what is in their mind may differ from that what is in other people's minds (Perner & Lang, 1999). Prior work exploring children's and teenagers' privacy perceptions and management indeed suggests differences between younger and older age groups. For instance, Feng and Xie (2014) found that children are less

concerned about their data being collected by marketers than their parents are. Moreover, Turow and Nir (2000) found that children between 10 and 17 years old were much more likely to provide sensitive personal data to commercial sites in exchange for a free gift than their parents. In the context of social network sites, teenagers also reported employing fewer privacy settings than adults (Christofides, Muise, & Desmarais, 2012).

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

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

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

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

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

Being literate is however a stipulation for being able to make these cost-benefit trade-offs. Media literacy that covers different types of literacy, such as privacy and advertising literacy, encompasses a variety of skills that people need to have to be able to critically analyse messages in audio, print, video, and multimedia (Hobbs, 1999) and has been put forward by scholars as an empowering element in engaged citizenship (Mihailidis & Thevenin, 2013). The acquirement of such literacy enables individuals to make rational decisions and have the cognitive tools to interact with all types of media, both online and offline (Masterman, 2003). Having overall knowledge and insights into the business models that companies use may also raise awareness about privacy harms and is necessary for individuals to make evaluations and consolidated decisions on disclosure (Trepte et al., 2015). That is, knowing that a company will use personal data for commercial purposes may evoke engagement in privacy protective behaviour. This may be problematic when it comes to children because they have different levels of developmental and cognitive capabilities than adults have and may thus not possess such know-how and data protection abilities. For instance, in the context of advertising, it was found that at the age of 12, children have still not developed an adult-like understanding of advertisers' selling and persuasion intentions (Rozendaal, Buijzen, & Valkenburg, 2010). Also, they sometimes overvalue their understanding of mar-

keting practices and, as a result, eventually engage in more risky behaviours (Shin, Huh, & Faber, 2012). Beside their underdeveloped privacy literacy, their cognitive control is not yet entirely matured and may even get surpassed by affective reward processes too. This may make them biased toward appraising the benefits that are given in return for data, and may lead to greater willingness to disclose data and smaller motivation to protect their privacy (Walrave & Heirman, 2013; Youn, 2009).

3. This Study

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

4. Method

4.1. Study Design

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

4.2. Participants

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

4.3. Procedure and Interview Guide

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

Table 1. Participants' demographic information.

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

Note: Fictive names are used to guarantee anonymity.

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

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

4.4. Data Analysis

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

5. Results

5.1. Children's Coping Strategies

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

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

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

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

5.2.1. Incomplete Understanding of How Data Collection Practices Work

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

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

5.2.2. Some Level of Privacy Consciousness

Although children may not spontaneously understand the consequences of data practices for their online privacy, they did seem to hold a certain level of privacy

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

5.2.3. Positive Attitude toward Use of Personal Data

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

5.3. Parents' Coping Strategies

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

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

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

5.4. Parents' Privacy Literacy and Perceptions of Data Practices

5.4.1. Incomplete Understanding of How Data Collection Practices Work

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

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

5.4.2. Concerns about Children's Personal Data

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

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

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

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

5.4.3. Mainly Negative Attitude toward Use of Personal Data

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

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

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

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

5.4.4. Perceived Lack of Control and Complacency

Some parents believed privacy protection to be out of their control, especially in the case of implicit data practices. This is demonstrated by five parents, including Gabriela (41): 'What can we do about it? I don't know. If I could, I'd love to protect my child but we don't have any control.' She allocated this lack of control to the ability of businesses to track down individuals' actions anytime users go online, 'Because, once you step on the internet, what you are searching, what you are doing….It's

somewhere memorised. It's something that they can always check' (Gabriela, 41). Moreover, while some parents knew cookies could be erased, they did not always act upon this. Put differently, together with the fact that they are insufficiently informed about effective privacy protective strategies and show a low perceived self-efficacy, they also find it too effortful to actually take appropriate actions.

6. Conclusion

6.1. Discussion

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

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

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

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

When it comes to protecting their kids' privacy, the interviewed parents mainly engaged in restrictive mediation strategies (e.g., imposing them to use a website that does not request personal data), and again, did mainly so in the case of explicit data practices. Some parents also engaged in instructive mediation strategies (e.g., explicitly explaining the potential threats to their children)

when their kids seem to be ready in terms of age and internet abilities. A possible explanation for the principal use of restrictive mediation strategies can be found in Lee's study (2013). His study found that the younger the child is, the more often parents use diverse restrictive strategies. This may be because young children have still not fully developed skills to cope properly with online risks independently and therefore mainly benefit from external guidance and restrictions.

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

6.2. Managerial and Public Policy Implications

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

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

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

6.3. Limitations and Suggestions for Future Research

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

As employing users' personal data for the creation of personalised advertisements is a common business prac-

tice, further research can also benefit from more comprehensive insights into the impact of these advertisements among children. In particular, future work could look into how personalisation influences children's brand and ad responses, and how media (or privacy) literacy can empower them when they are confronted with different types of personalised advertisements.

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

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

Acknowledgments

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

Conflict of Interests

The authors declare no conflict of interests.

Supplementary Material

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. M. Jones & M. Tscheligi (Eds.), *Proceedings of the ACM on Human–Computer Interaction* (pp. 1–21). New York, NY: Association for Computing Machinery.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In *Reforming European Data Protection Law*, *2015*, 333–365.

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

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

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

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

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

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

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

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

About the Authors

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

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

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