Media and Communication (ISSN: 2183–2439)
2022, Volume 10, Issue 1, Pages 317–328
https://doi.org/10.17645/mac.v10i1.4704

Article

Exploring Teenagers' Folk Theories and Coping Strategies Regarding Commercial Data Collection and Personalized Advertising

Sanne Holvoet [1], Steffi De Jans [1], Ralf De Wolf [1,2], Liselot Hudders [1,*], and Laura Herrewijn [3]

[1] Department of Communication Sciences, Ghent University, Belgium
[2] imec-mict-UGent, Ghent University, Belgium
[3] Department of Management and Communication, AP University of Applied Sciences and Arts Antwerp, Belgium

* Corresponding author (liselot.hudders@ugent.be)

Submitted: 15 July 2021 | Accepted: 27 October 2021 | Published: 29 March 2022

Abstract

New data collection methods and processing capabilities facilitate online personalization of advertisements but also challenge youth's understanding of how these methods work. Teenagers are often unaware of the commercial use of their personal information and are susceptible to the persuasive effects of personalized advertising. This raises questions about their ability to engage in privacy-protecting behaviors. This article examines teenagers' coping responses to commercial data collection and subsequent personalized advertising, considering their limited knowledge. Ten focus groups with 35 teenagers aged 12–14 were conducted. The findings show that teenagers hold certain folk theories (i.e., incomplete and/or inaccurate representations of reality) about how and why their personal information is being collected for commercial purposes (e.g., commercial data collection is unavoidable or all principles of privacy statements are the same). Their coping responses regarding commercial data collection (e.g., limiting information disclosure or refusing to accept privacy policies) and personalized advertising (e.g., trying to change settings or avoiding interaction) are often based on these folk theories and embedded in their everyday practices. Despite teenagers' efforts, we argue that their responses might not always be effective. Implications for educators, advertisers, and policymakers are discussed.

Keywords
commercial data collection; folk theories; personalized advertising; privacy management; teenagers

Issue
This article is part of the issue "Digital Child- and Adulthood: Risks, Opportunities, and Challenges" edited by Claudia Riesmeyer (LMU Munich), Arne Freya Zillich (Film University Babelsberg KONRAD WOLF), and Thorsten Naab (German Youth Institute).

© 2022 by the author(s); licensee Cogitatio (Lisbon, Portugal). This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

1. Introduction

Teenagers spend a vast amount of time online using different devices and platforms (Ofcom, 2021), during which they are subjected to commercial data collection practices ranging from explicit to implicit. For example, teenagers often freely give up their personal information when participating in online games and contests or when using social media, including demographics, pictures, videos, and status updates (Pangrazio & Selwyn, 2019; Stoilova, Livingstone, & Nandagiri, 2019). However, disclosing information does not always happen intentionally, as some information is being collected automatically (e.g., technical details; Pangrazio & Selwyn, 2019). Indeed, teenagers disclose a vast amount of personal data in a more implicit way, without their overt awareness or consent. For instance, data-tracking technologies trace their online behavior (e.g., through cookies; Boerman et al., 2017), and profiling activities automatically process information to predict their interests (Lievens & Verdoodt, 2018).

Advertisers, in turn, use the collected information for commercial purposes, such as personalized advertising. Thus, teenagers may encounter online advertisements that are based on their age, gender, previous browsing behavior, or predicted interests (Youn & Shin, 2019). Advertising companies mostly lack transparency about how and why they gather personal information (Boerman et al., 2017; van der Hof, 2017). Unsurprisingly, teenagers are therefore not fully aware of the preceding data collection practices and the personalization tactics (Pangrazio & Selwyn, 2018; Stoilova et al., 2020; Stoilova, Nandagiri, & Livingstone, 2019; Zarouali et al., 2020). Accordingly, previous research has shown that teenagers have difficulty monitoring and dealing with their personal information being collected by advertisers (Stoilova, Livingstone, & Nandagiri, 2019; Youn, 2009). In addition, the subsequent personalized advertising they are exposed to improves (young) teenagers' attitudes and behavioral intentions toward the advertisements, but impedes critical processing (Daems, De Keyzer, et al., 2019; van Reijmersdal et al., 2017; Walrave et al., 2016; Zarouali et al., 2017).

Literature on consumers' responses to personalized advertising and online data collection practices often draws on privacy calculus theory, which suggests a trade-off between the benefits and risks related to these practices (Youn, 2009; Youn & Shin, 2019). Recent research, however, has shown that teenagers are willing to provide their personal information to online marketers in exchange for commercial incentives (Daems, De Pelsmacker, et al., 2019; Walrave & Heirman, 2012) and that their engagement in privacy-protecting strategies regarding targeted advertising is low (Selwyn & Pangrazio, 2018; Zarouali et al., 2020). Moreover, teenagers seem to find the social value of participating online more important than the potential risks related to the collection and use of their personal information (Lapenta & Jørgensen, 2015).

Teenagers' high levels of participation online and their willingness to make information trade-offs, combined with a limited understanding of implicit and explicit data collection methods, begs the question to what extent they protect their personal data from commercial usage and what impact this has on their responses to personalized advertising. Internet users may have developed intuitive or folk theories (i.e., incomplete and/or inaccurate representations of reality) to explain how something works, which may affect how they cope with digital systems (DeVito et al., 2017; Gelman & Legare, 2011). As they lack actual knowledge, it is important to understand people's beliefs when we want to understand their coping behaviors (Toff & Nielsen, 2018). To our knowledge, no previous study has looked into the way teenagers develop folk theories about the current data ecology and how this is connected to their coping strategies in the context of personalized advertising. Herein, we address this gap in the literature and explore teenagers' coping responses to implicit and explicit data collection and personalized advertising, whilst considering their folk theories. We organized 10 focus groups with 35 teenagers aged 12–14 to talk about their experiences with these practices.

2. Theoretical Background

Consumers' coping responses to deal with personalized advertising and online data collection practices have often been examined through the lens of privacy calculus theory (Baek & Morimoto, 2012; Youn & Kim, 2019). This theory posits that users weigh the benefits and risks (or costs) related to personalized advertising and information disclosure (Hart & Dinev, 2006). Depending on the outcome, they may respond positively or negatively toward the personalized advertisement or data collection attempt. As such, Youn and Shin (2019) showed that 13- to 19-year-olds engage with personalized advertising when they perceive the benefits (e.g., relevance) are greater than the risks (e.g., intrusiveness). Conversely, teenagers avoid personalized advertisements when this trade-off turns out negative. In another study, Zarouali et al. (2017) revealed that teenagers aged 16–18 try to protect their privacy by adopting a skeptical stance toward retargeted advertisements when concerned about online companies using their personal information. Research on teenagers' coping with commercial data collection attempts—which precede their exposure to personalized advertising—showed that teenagers rely on this risk–benefit trade-off as well when asked by commercial parties to share their personal information (Youn, 2009). In this way, teenagers can be persuaded to disclose their personal details in exchange for, for example, a chance to win a smartphone (Daems, De Pelsmacker, et al., 2019) or commercial incentives (Walrave & Heirman, 2012).

Perceptions of privacy risks and the related concerns about the commercial use of personal information are—given its impact on the risk–benefit trade-off—often referred to as a predictor of privacy-protective behavior (Baruh et al., 2017). However, the "privacy paradox" phenomenon describes a discrepancy between concerns and actual behavior (Kokolakis, 2017). Particularly, consumers are not necessarily more likely to engage in privacy-protective behavior when they are concerned about privacy risks (e.g., Acquisti et al., 2015; Lutz et al., 2018). For instance, Zarouali et al. (2020) recently showed that teenagers' (aged 13–17) engagement in privacy-protecting strategies in the context of targeted advertising is low, although the teens were concerned about the collection and use of their personal information. Conversely, other studies showed that teenagers have little concern at all about personalized advertising or the preceding data collection (Lapenta & Jørgensen, 2015; Pangrazio & Selwyn, 2018). In fact, they often find the social value of participating online increasingly important and downsize the potential risks related to it, which leads them to accept the commercial data collection without being worried about their privacy (Lapenta & Jørgensen, 2015).

This is where the relevance of knowledge for privacy-protective behavior comes in. Particularly, it is important that internet users are aware of commercial companies collecting and handling their personal information and how these data practices work (Baruh et al., 2017; Trepte et al., 2015). This knowledge raises awareness of the risks and potential consequences of sharing their personal information (Trepte et al., 2015), enabling and encouraging consumers to make informed risk–benefit decisions and consequently to apply privacy-protective measures (Baruh et al., 2017). As such, Selwyn and Pangrazio (2018) discussed that teenagers will not be motivated (and neither will they be concerned) to act if they do not see the commercial use of their personal information as a problem. Previous research indeed showed that young people generally do not perceive their personal information as valuable to advertisers and are not fully aware of the information third parties gather or commercial repurposing of this information (Lapenta & Jørgensen, 2015; Pangrazio & Selwyn, 2018; Stoilova et al., 2020; Stoilova, Nandagiri, & Livingstone, 2019; Zarouali et al., 2020). Given teenagers' limited understanding, the current study begs the question to which extent teenagers are capable of rational decision-making regarding their personal information and their exposure to personalized advertising.

Yet, lacking actual knowledge of how data collection practices and advertising personalization work does not mean that teenagers are completely unaware of how their personal information is being commercially exploited. Teenagers may as well have some mental models of data collection and personalized advertising, based on their personal experiences, perceptions, and understandings (Jones et al., 2011). Recently, academia has increasingly focused on how people form "algorithmic imaginaries" (i.e., how they imagine, perceive, and experience algorithms; Bucher, 2017) or "folk theories" about algorithms (e.g., DeVito et al., 2018). DeVito et al. (2017, p. 3165) define these theories as "intuitive, informal theories that individuals develop to explain the outcomes, effects, or consequences of technological systems, which guide reactions to and behavior towards said systems." Folk theories are, however, incomplete and simplified assumptions of reality and may thus be incorrect, which means that they may lead to erroneous decision-making (Wash, 2010). In the context of the current study, consumers' misperceptions of commercial data collection and personalized advertising may thus undermine informed and effective decisions on privacy-protective behavior (Acquisti et al., 2015; Boerman et al., 2017; Yao et al., 2017).

To the best of our knowledge, previous research has not considered teenagers' folk theories for understanding their everyday coping behaviors. The current study aims to examine teenagers' engagement in privacy-protective behavior considering their limited knowledge of the current data ecology and ability to engage in rational decision-making regarding their personal information. This study is particularly interested in how teenagers develop folk theories about online data collection and personalized advertising and how these folk theories are connected to their use of privacy-protection strategies.

3. Methodology

3.1. Study Design

Focus group discussions were conducted with teenagers. Data were collected in three waves, and we adopted an iterative approach in which the information learned from the previous wave was used to revise the interview material for those following. Two researchers moderated the discussions.

3.2. Participants

Ten focus groups were conducted with 35 teenagers (20 girls, 15 boys) aged 12–14. Appendix I (see Supplementary File) shows an overview of the focus groups' composition, the participants, and their demographics. All teenagers indicated being familiar with different media devices and being active on multiple social media platforms. They received a voucher for an online store for their participation.

The first two focus groups were conducted in March 2020 (wave 1). Participants were recruited from two secondary schools in Flanders (Belgium), and the discussions took place after school hours in a classroom. Thereafter, the data collection was paused when schools in Belgium physically closed mid-March 2020 due to the Covid-19 pandemic. In Summer 2020, we resumed data collection by organizing online focus groups using Microsoft Teams (wave 2). We organized four smaller focus groups through snowball sampling. Due to the second lockdown in November 2020, the study was paused again. Data collection resumed in January 2021 after recruiting teenagers from a third secondary school (wave 3). With a teacher's assistance, we organized four more online focus groups.

3.3. Procedure and Topic List

First, ethical consent was obtained from the ethics committee of the researchers' university faculty. Consent was also requested from one of the teenagers' parents or legal guardians, and teenagers were informed about the study's purpose before agreeing to participate. The face-to-face conversations lasted no longer than 1.5 hours. The online focus groups took approximately one hour. All conversations were recorded with both audio and video.

The (semi-structured) topic guide was updated after each data collection wave (cf. iterative research design). Each conversation began with the researchers introducing themselves, explaining the study's purpose, and ensuring confidentiality and anonymity. In the first two waves, we mainly asked questions to explore teenagers' understanding, attitudes, and experiences regarding the collection and use of their information for personalized advertising. Other themes such as the business model of service providers, giving (informed) consent, and control over personal information were discussed as well. Based on the data of these waves, we inferred various folk theories and coping responses regarding the topics of interest. In the third wave, we further elaborated on these findings and focused on teenagers' coping strategies.

To facilitate the focus groups, we prepared some tasks and materials. For example, the respondents were asked to visit their Instagram profile (or another app) and to scan the ads they saw (cf. social media scroll back method; Robards & Lincoln, 2019). We asked whether their newsfeed advertisements were personalized and if yes, how this works. Furthermore, we showed some videos explaining explicit (i.e., voluntary information disclosure) and implicit (i.e., unconscious information sharing) data collection practices. A few examples of personalized advertising (e.g., location targeting, retargeting) were shown as well. Each focus group ended with the discussion of specific statements, such as "apps and websites have the right to collect and use my personal information." The topic list of wave 3 can be found in Appendix II (see Supplementary File).

After each data collection wave, the focus groups were transcribed, anonymized, and analyzed using NVivo software. To structure the data, the first author developed a coding scheme using both deductive (theory-driven) and inductive (data-driven) thematic analysis (Braun & Clarke, 2006; see Appendix III, in the Supplementary File). The main codes (i.e., knowledge and perceptions, attitudes, coping) and categories (i.e., personalized advertising, explicit data collection, implicit data collection, and informed consent) were deductively defined based on prior literature and the themes in the topic list. Following an inductive approach, we were also mindful of recurring patterns and new information. These codes were attached to the information in the transcripts. An iterative approach was taken as well during the coding procedure, so the data and inductive codes were reconsidered, restructured, and redefined after each data collection wave.

4. Results

4.1. Folk Theories

We found that teenagers hold four main folk theories that help explain how they think about and cope with online data collection and the subsequent personalized advertising. These folk theories encompass beliefs that: (a) data collection is unavoidable, unclear, and unrelated to advertising; (b) personal information is handled by real people; (c) all the principles of privacy statements are the same; and (d) data collection and processing is an individual responsibility. Anonymized quotes in support of the results can be found in Appendix IV (see Supplementary File). When presenting quotes from the interviews, we'll use F# to signify to which focus groups that interviewee belonged to.

4.1.1. Personal Information Collection is Unavoidable, Unclear, and Unrelated to Advertising

The respondents generally agreed that the collection of personal information is a standard practice among commercial companies and therefore unavoidable. They were convinced that they cannot do anything online without disclosing some type of personal information to an app or website. However, the respondents struggled to give clear answers when we asked how their data is collected by advertisers to create personalized advertisements. Most respondents indicated more implicit data collection methods and were aware that their online activities are being tracked by cookies. However, they were unable to explain how these cookies work:

> F4 Interviewer: Do you all get to see the same advertisements?
>
> Pascal (13): No, I don't think so.
>
> Mason (12): Isn't that what cookies are for?
>
> Pascal: Yes!
>
> Mason: If you accept cookies on a certain website, don't you get advertising related to that?
>
> Interviewer: What are those cookies exactly?
>
> Mason: I don't know about that.

Based on their previous experiences, the respondents did claim cognizance of how their surfing behavior shapes the advertisements they see: "I notice that when I search something on Google that I suddenly get advertising about that, or something related to that" (F3 Zoey, 14).

Some respondents also mentioned other implicit data collection methods, such as the usage of location details to personalize advertising and eavesdropping through built-in microphones. Most respondents, however, did not believe the last practice to be true. The respondents rarely mentioned more explicit data collection methods for personalized advertising. They believed that websites and apps request their information for non-commercial purposes, such as inputting their age to be allowed to use social media or requesting interests to show relevant non-commercial content: "I know that when you create an account on TikTok that you have to indicate your interests….I think this is to determine the videos that you get to see" (F3 Zoey, 14).

Interestingly, some respondents believed that their personal information could be collected through the online behavior of their friends: “If you have many friends who live close and turned their location on, I think that they [companies] can find out your location as well” (F1 Ellen, 12).

4.1.2. Personal Information is Handled and Read by Real People

In the second folk theory, the respondents assumed that the information disclosed to commercial parties is handled and read by real people—and not processed by algorithms as it is in reality. When discussing commercial parties’ information practices, respondents referred to “them” as the people working for these companies. Additionally, they voiced ideas about other things that could happen with the data when those people have other intentions, such as lurking or using information for burglary or hacking purposes. Even after explaining how this is an automatic, anonymous process, the respondents seemed to have difficulties relinquishing their initial reasoning: “But they have all your information, and you don’t know what they do with that. So, if they want, they can also misuse it” (F9 Willow, 13).

4.1.3. All Principles of Privacy Statements Are the Same

The respondents were generally aware of the privacy statements they are exposed to when visiting websites, downloading apps, and creating social media profiles. They realized that by accepting these statements, they give permission to these platforms. Most respondents were also aware that they automatically agree with the privacy policies of social media sites when signing up. However, they do not know precisely what they give permission for and referred to the content of privacy statements as “having something to do with privacy.” The respondents were not aware that these statements also include permission for using their data for commercial purposes and, hence, for personalized advertising. Additionally, some respondents assumed that the same information and principles are written down in every privacy statement and thus didn’t perceive them as having added value. Others questioned this but could not indicate any differences between different services’ privacy policies.

> F4 Pascal (13): I didn’t know it contained that. But I did know a bit about the privacy stuff of Instagram, for example, but I didn’t know that it goes to advertisers…. [About privacy policies] It’s all about the same, I think….There are not going to be many differences.

4.1.4. Data Collection and Processing is an Individual Responsibility

When respondents were informed by the moderators that they give companies permission to use their personal information to implement personalized advertising by accepting privacy statements or signing up on social media, they justified these practices by showing understanding concerning advertisers. They reported that it is their own responsibility that they are involved with these practices as it was their own choice to agree with the terms, without informing themselves of what they give permission for. In a way, they blamed themselves for not being aware of certain data collection and personalization practices and now resign themselves to it because they feel that they should have known better.

> F2 Mila (12): You have chosen it for yourself.
>
> F1 Sam (14): It’s fine for me [advertisers processing his personal information]…because you’ve agreed with it.
>
> F8 Interviewer: You also give permission for the use of your personal information for advertising when agreeing with the privacy policy. How do you feel about this way of giving consent, knowing that most people don’t read this privacy policy?
>
> Leah (13): It’s in there, so it’s up to you if you want to read it. If you don’t want to read it, then that’s your own fault.

4.2. Coping Strategies

In what follows, we provide an overview of the teenagers’ coping mechanisms towards (a) personalized advertising, (b) explicit data requests, (c) implicit data collection, and (d) informed consent and permission requests and how the previously mentioned folk theories shaped our respondents’ reasoning and practices.

4.2.1. Coping with Explicit Data Requests

When their personal information is explicitly requested, the respondents only give up the information that is required to continue their online activities. Cues such as a textual disclosure indicating what information is required or asterisks following the entry fields inform and guide them in this. Additionally, they make a trade-off between the information they do and do not want to disclose:

> F1 Interviewer: Which information do you give up?
>
> Sam (14): Everything you need to fill in.
>
> Finn (12): Yes, everything that is needed to make it work.
>
> Interviewer: And how do you know which information is needed?
>
> Finn: If there’s an asterisk next to it.

> F8 Lucy (13): I try to choose. Sometimes they ask either your email address or place of residence or phone number, and then usually I give my email address because I don't like to give my phone number.

Additionally, teenagers assess the trustworthiness of an app or website to determine their information disclosure (with more trust resulting in more information disclosed). They are most often guided by a gut feeling, but some respondents recognize signals referring to suspicious data requests (e.g., the number of questions or website reviews). Their familiarity with the website or brand also plays an important role, as respondents are more likely to trust well-known platforms. However, their information disclosure to popular social media sites still depends on the sensitivity of the information requested.

> F10 Nikki (12): I wouldn't disclose where I live [when making an account] if I don't trust it.
>
> Interviewer: Why wouldn't you trust it?
>
> Nikki: Just because you never know what they will do with it.
>
> F9 Arthur (12): To Snapchat and all those other well-known apps, I would just give my personal information because you know a lot of people are on it, and it's reliable. But for other apps, that not so many people use, I would not give my personal information so quickly.

Peers are important references for this trustworthiness as well, as teenagers often imitate the behavior of friends and do not expect their friends to engage in risky behavior. Two respondents let their parents check the reliability of a website or app: "My friend did it as well, so I trust that, and there has nothing bad happened to them" (F7 George, 12).

The above findings show that respondents have already developed some coping mechanisms to control their personal information disclosure. They are unlikely to give additional information if not required, as they do not understand the necessity. Their information disclosure is mainly based on an assessment of trust in the data requesters. Particularly, they consider whether they can trust a company with their information, specifically the people working for that company, as they believe that their personal information is handled by real people and may thus fall in the wrong hands (cf. folk theory 2). This means, however, that when they trust the app or website, they are less likely to engage in protective behavior.

4.2.2. Coping With More Implicit Forms of Data Collection

We identified three coping strategies concerning more implicit forms of data collection. First, some respondents believed that they could protect their personal information from advertisers and commercial companies by having a private account:

> F2 Jonas (12): You disclose your personal information by uploading photos on Instagram when you have a public account. They [commercial company behind the app] can't see it when you have a private account…. I think it is allowed to do this [advertisers collecting and using personal information] with a public account, but with a private account, I think it is illegal.

Second, a respondent in the first focus group assumed that advertisers do not have much of his personal information because of infrequent social media usage. When we discussed in the following focus groups whether using less social media could be a coping response to avoid personal information from being collected, most of the respondents agreed but were not inclined to actually do this: "Yes, I think so! But I'm not sure if that's something for me to do" (F9 Emily, 13).

Third, some respondents thought that they could avoid online tracking by simply not logging in on a website or social media app. When asked how this may help them avoid being subject to advertisers, they felt that they would not get advertisements based on their interests in this way.

> F7 George (12): Sometimes, you don't need to log in—you can skip that.
>
> Interviewer: How would that help [to avoid data collection]?
>
> George: You don't get to see advertising that's relevant to you then.
>
> Willow (13): On Google, I notice that when I log out, I get to see totally different advertisements.

Such coping responses were, however, not supported by all the respondents. For others, it was unclear whether having a private account, not logging in, or using less social media would prevent their personal information from being collected by commercial companies. While some respondents questioned the effectiveness of these strategies, others felt that commercial personal data collection is unavoidable (cf. folk theory 1).

The idea that their personal information is handled by real people (cf. folk theory 2) explains why respondents believed that setting up a private account protects them from unwanted audiences. However, private accounts do not guarantee that personal information is being collected and used to show advertisements. Additionally, because most respondents are aware that they give permission to commercial companies when signing up for social media (cf. folk theory 3), they may engage in coping responses to evade giving permission. As such, they may not log in on websites, believing that companies will not track them. Actual data collection, however, happens when users are not logged in as well. Moreover, respondents believed that it is guaranteed that companies collect and process personal information (cf. folk theory 1) and that they are responsible for deciding whether they want to participate in these practices by using social media or not (cf. folk theory 4).

4.2.3. Coping With Informed Consent and Permission Requests

Although none of the respondents read privacy policies, terms of services, or cookie disclosures, they mostly accept them. Few respondents would cope critically with permission requests by refusing to accept cookies or giving permission to their data:

> F1 Luke (13): I'm not really careful with that. I usually agree because I know what it is.
>
> F7 Lenny (13): I first check which website it is and if I know I can trust it, such as [*Het Nieuwsblad*; regional news site], then I accept the cookies. But if the lock is open, then I will not accept it.
>
> Interviewer: What do you mean with that lock?
>
> Lenny: In this way, my computer shows whether the website is secured or not.
>
> Interviewer: And what if you can't continue if you don't accept the cookies?
>
> Lenny: I just go to another website.

The main reason why respondents agree with privacy policies without reading is because they feel obligated. Hence, most respondents believe that it is impossible to disagree if they want to use an app or social media platform. Similarly, respondents accept cookie policies so they can proceed and treat these policies as obligatory passage points. This reasoning is related to the assumption that the collection of personal information is unavoidable (cf. folk theory 1): "You can only accept. You can choose to accept or to read more privacy information, but you can never refuse" (F8 Leah, 13).

Additionally, respondents do not understand the importance of reading the privacy policy on every website or app they visit, since they believe that every policy is the same (cf. folk theory 3). Similarly, they believed that cookies are the same for every website and therefore do not understand why it would be necessary to accept disclosures repeatedly for every website and app:

> F1 Sam (14): Maybe I did read that [privacy policy once] once, but it's the same principle everywhere.
>
> F6 Bella (12): I believe that for some people, it might be useful, but I think that others might not understand why it [cookie disclosures] still appears if they always accept it anyway.

Respondents' critical coping is again based on their trust perceptions, which arise from the idea that the people behind the app or website may access their personal information (cf. folk theory 2). Particularly, some respondents first look at whether the website is secure before accepting cookies.

4.2.4. Coping With Personalized Advertising

The respondents find retargeted ads—based on their online behavior—less annoying than non-retargeted advertisements and are therefore less inclined to resist them. Some respondents, however, do their best to avoid interaction with advertisements to protect themselves from being targeted further: "I never like sponsored posts because if I like that, I know that I will get it again, and before you know, I will get to see these advertisements each time I look at Instagram" (F2 Jonas, 12).

The respondents had less experience with other personalization practices. We gave some examples of personalized advertising based on different types of data. First, we displayed social advertising (i.e., an advertising format that leverages friends as endorsers). While some teenagers said that they would not mind this, others would investigate how to avoid this (e.g., by changing settings):

> F1 Sam (14): I wouldn't find that a disaster because I have probably given permission for that in the general conditions, but I wouldn't appreciate it either. I would just dislike it [the brand] again.
>
> Luke (13): I would look if I can turn that off, but if I can't find how to do that, I would probably leave it like that.

While the respondents are unlikely to do something if their profile information is used, some reported being motivated to react protectively against personalized advertisements based on "creepy" data sources (e.g., location data or chat history). They then might look for the settings to disable such advertising practices, but they questioned their own capabilities to do so. Other teenagers would not mind their information being used to create targeted advertising for a well-known or trusted brand:

> F8 Lucy (13): I would see if there is a way to disable this…but I wouldn't know how to do this. Because they have this information, they can read your chat messages, so I don't think there is much you can do about it.…I wouldn't get issues with that [location-based ads] because okay, they have found out where

> I am based on my location, but still, it's just from McDonalds, so I wouldn't mind that very much.

The findings showed that the respondents do little to actively cope with personalized advertising, as they do not link the collection of their personal information to advertising (cf. folk theory 1) and are mostly unaware of how personalized advertising works. When expressing their concerns regarding privacy-invasive personalized advertisements (e.g., based on location or chat history), the respondents again considered that their personally identifiable information is processed by real people (cf. folk theory 2), whereby they are more likely to adopt a critical stance toward the ad. That being said, even with awareness of personal information usage, they may neglect to respond because they perceive they are responsible for being exposed to these ads (cf. folk theory 4). Specifically, if they were aware that they had given permission for such practices when signing up or accepting the privacy policy, they felt that such advertisements are part and parcel of the process and that they should have known better.

5. Conclusion

Previous research has shown that teenagers' knowledge of personalized advertising and the preceding commercial data collection is limited (e.g., Stoilova, Livingstone, & Nandagiri, 2019; Zarouali et al., 2020). The current study delves deeper into teenagers' ways of thinking and offers a more nuanced understanding. Specifically, our study illustrates how teenagers hold different folk theories that—partially—explain their coping responses.

The first folk theory assumes that the collection of personal information by commercial companies is unavoidable. Therefore, teenagers feel that they have little control over commercial data collection practices, which aligns with the feeling of powerlessness found in previous research (e.g., Pangrazio & Selwyn, 2018; Stoilova et al., 2020). Commercial data collection practices in the context of personalized advertising are unclear for teenagers, causing them to do little in response to personalized ads. However, they demonstrated a certain awareness of the use of their online behavior for targeted advertising and therefore avoid interaction with targeted advertisements. Hence, teenagers may cope with personalized ads when they are aware of what happens to their personal information. Yet, most teenagers still perceive targeted advertisements as being more beneficial than irrelevant advertisements, which is in agreement with previous research on the effectiveness of personalized advertising (Kelly et al., 2010). When further discussing other personalized advertising formats, the teenagers sometimes disagreed with certain practices (e.g., using data from creepy data sources) and indicated that they would want to adapt the settings to disable this. However, they immediately reflected on their capability to do this as they did not know how to control personalized advertising and therefore leave it at the default settings. In agreement with previous research (e.g., Ham, 2017; Zarouali et al., 2018) we argue that teenagers' lack of self-efficacy (i.e., one's confidence in their ability to successfully change the privacy settings) may be a barrier to actually adopting privacy-protective strategies regarding personalized advertising.

The second folk theory purports that personal information is handled and read by real people. Hence, teenagers link a social context to commercial data collection. As discussed by Stoilova et al. (2020) and Desimpelaere et al. (2020), this may lead teenagers to think that companies have the same values as someone they personally know and to adopt the same coping responses regarding their social privacy (i.e., regarding friends or parents). Our study supports this by showing that teenagers believe that creating a private account may protect their information from commercial parties. This assumption causes teenagers to base their privacy-protective decisions on perceptions of trust, as has also been shown in previous research (e.g., Walker, 2016). Particularly, our study reveals that teenagers have developed some trust mechanisms on which they rely to assess the environment in which they receive information or permission requests. Accordingly, they will determine their information disclosure and acceptance of privacy policies and cookie disclosures. Perceptions of trust may also develop from teenagers' gut feelings, which questions the effectiveness of these mechanisms. Interestingly, teenagers indicated that their coping with personalized advertisements depends on the trustworthiness of the brand being advertised, while on social networking sites it is the platform itself that is responsible for managing users' data and targeting them with the advertisement. Hence, wrong assumptions may lead to ineffective decision-making.

Teenagers feel forced to accept privacy statements and cookies if they want to participate online, which is a well-known phenomenon (e.g., Lapenta & Jørgensen, 2015; Pangrazio & Selwyn, 2018; Stoilova et al., 2020). However, our study provides further insights into teenagers' reasoning about information policies. The third folk theory reveals that teenagers believe that every privacy statement contains the same principles, and that informed consent is the same for every website and app. Resultingly, they do not deem it necessary to read cookie disclosures and privacy policies. Accepting cookies or privacy policies is a part of their daily routines and is thus not perceived as a meaningful coping strategy by teenagers. They agree with it anyway because they want to continue their online activities, of which the rewards are more important than their privacy (cf. privacy calculus theory). In addition, the teenagers indicated that privacy statements are too complex for them to understand (cf. self-efficacy), which stops them from actually getting into it as well. Moreover, some teenagers indicate they perceive signing up for and using a website or app as an automatic way of consenting. This perception may guide teenagers' coping behavior, for example, when they decide not to sign up or not to use a website or app to avoid their personal information being collected. However, it is worrisome that teenagers perceive implied consent and click-through agreements as normal, given that they are not adequately informed about what they involve.

When teenagers were told that they give consent for personalized advertising practices by accepting cookies and privacy policies, they were not bothered. The fourth folk theory shows how they justify advertisers' practices, as they feel that it is their own responsibility and decision to consent with data collection and exposure to personalized advertising without being well-informed. They feel like they should have known better, and therefore resign themselves to it. Rather paradoxically, they see commercial information collection as unavoidable (cf. folk theory 1) but something they need to decide for themselves. Additionally, this study shows that this individual responsibility may discourage teenagers from engaging in purposeful coping. Teenagers were sometimes unlikely to engage in privacy-protecting strategies toward these practices, as they felt that advertisers had the right to do so because they consented when signing up or agreeing with the terms of service. This shows how teenagers perceive their privacy in a commercial context as a property right, which can be given away to advertisers (see De Wolf et al., 2017).

5.1. Limitations and Further Directions

This study has some limitations that provide directions for further research. First, teenagers' folk theories are based on the information they could retrieve from memory and may be subjected to biases (see Podsakoff et al., 2003). In addition, there may be a gap between teenagers' intentions to cope with personalized advertising and online data collection and their actual behavior (see e.g., Norberg et al., 2007). Therefore, we suggest that teenagers' coping behavior regarding personal data requests, cookies, and privacy policies, and personalized advertising messages may be further examined by collecting data through participant observation. Furthermore, research may extend our work by further examining the determinants of teenagers' knowledge and coping behavior (e.g., self-efficacy), in this context.

Second, this study did not discuss the available control functions that allow teenagers to cope with these practices (e.g., turning personalization off). Further research may explore why teenagers are unaware of these options or why they do not succeed in adopting them. Moreover, it would be interesting to examine the extent to which teenagers have a need for such tools. They often indicated being powerless or indifferent regarding data collection practices, but it is unclear to what extent they desire more transparency or better control options.

Lastly, the study used a small convenience sample, which may be biased, as some focus groups had to be conducted online (due to the Covid-19 pandemic). The sample consisted of Flemish teenagers who were easy to reach and is therefore not statistically representative. Still, our study provides some nuanced insights into teenagers' engagement in commercial privacy-protecting strategies.

5.2. Implications

These insights may be of interest to educators, the (advertising) industry, and public policies, which play an important role in teenagers' coping with personalized advertising and commercial data collection. First, we agree with previous researchers that it is important to educate teenagers about personal data flows and usage (e.g., through educational training or awareness campaigns), as knowledge may encourage them to actively engage in privacy-protecting behavior (Pangrazio & Selwyn, 2018). However, it was noticeable that even after an approachable explanation of personalized advertising tactics, the teenagers fell back on their folk theories when describing their responses to these practices. Hence, it is important to consider teenagers' intuitive theories and their capacities to understand these practices when developing educational programs. In addition, it is suggested that teenagers' self-efficacy should be strengthened so that they believe in their ability to successfully cope with personalized advertising, online data collection, and consent requests. However, teenagers could first be educated about how they can successfully change privacy and advertising settings, as they currently do not know how to do this.

While the industry and public policy may assume that teenagers are sufficiently informed to consent to personalized advertising and online data collection practices, the current study shows that their folk theories do not align with this; teenagers' understanding and practices contrast with the principles described by the General Data Protection Regulation (i.e., more transparency and control). As such, we believe that it is important to make teenagers better aware of the content and value of privacy policies or cookies disclosures. However, informed consent may still be impeded as those privacy policies are too difficult for teenagers—and even for adults—to understand, which suggests that policymakers should reconsider this strategy as a whole. For example, improving policies may not provide a solution if teenagers are still not intending to read them, but changing the way in which information is presented (e.g., through visual cues) may be a first step to protect vulnerable audiences more effectively. Additionally, the current control options to regulate their personal information are not perceived as useful or something they can hold on to. Hence, we encourage the industry to invest in and promote meaningful ways that give teenagers more control over their personal information and protect them from being manipulated by personalized advertising. Currently, there is little that advertisers do to properly inform or protect teenagers, which does not reflect ethical conduct.

In this regard, we believe that it is important to explore how the digital environment can trigger teenagers to routinely engage in privacy-protecting behavior and critically reflect on personalized advertising. We found that teenagers rely on trust perceptions to determine their information disclosure and agreement with privacy policies and that they are often guided by routines. Relevant authorities may, for example, invest in the development and implementation of cues that help them to guide their coping behavior. As a suggestion, an icon that discloses to teenagers what their personal information is being used for (e.g., for commercial use, to improve experiences) may help them decide whether they want to disclose their personal information. Additionally, we stress the need for a disclosure that informs teenagers about the implementation of personalized advertising based on their personal information as they are often unaware of advertising personalization. Current disclosures such as the AdChoices icon are not always noticed or clicked on by teenagers and are thus not sufficient for informing them. The advertising industry (e.g., the Digital Advertising Alliance) can reconsider these disclosures while taking into account teenagers' difficulties as addressed in this article.

Lastly, we could infer teenagers' folk theories are mostly based on their personal experiences. However, they draw on their parents and peers as well to form their theories and to determine their coping behavior. Hence, we suggest that these agents should be involved in the attempts to help teenagers cope with these practices.

Acknowledgments

This research was funded by the Research Foundation Flanders (FWO), grant number FWO.OPR.2017.0027.01 (funded doctoral fellowship of the first 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

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Baek, T. H., & Morimoto, M. (2012). Stay away from me: Examining the determinants of consumer avoidance of personalized advertising. *Journal of Advertising*, *41*(1), 59–76.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, *46*(3), 363–376.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, *20*(1), 30–44.

Daems, K., De Keyzer, F., De Pelsmacker, P., & Moons, I. (2019). Personalized and cued advertising aimed at children. *Young Consumers*, *20*(2), 138–151.

Daems, K., De Pelsmacker, P., & Moons, I. (2019). The effect of ad integration and interactivity on young teenagers' memory, brand attitude and personal data sharing. *Computers in Human Behavior*, *99*, 245–259.

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

DeVito, M. A., Birnholtz, J., Hancock, J. T., French, M., & Liu, S. (2018). How people form folk theories of social media feeds and what it means for how we study self-presentation. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, *2018*, Article 120, 1–12.

DeVito, M. A., Gergle, D., & Birnholtz, J. (2017). "Algorithms ruin everything": #RIPTwitter, folk theories, and resistance to algorithmic change in social media. In G. Mark & S. Fussell (Eds.), *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 3163–3174). Association for Computing Machinery.

De Wolf, R., Vanderhoven, E., Pierson, J., & Schellens, T. (2017). Self-reflection on privacy research in social networking sites. *Behaviour & Information Technology*, *36*(5), 459–469.

Gelman, S. A., & Legare, C. H. (2011). Concepts and folk theories. *Annual Review of Anthropology*, *40*(1), 379–398.

Ham, C.-D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, *36*(4), 632–658.

Hart, T., & Dinev, P. J. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1080/02650487.2016.1239878

Jones, N. A., Ross, H., Lynam, T., Perez, P., & Leitch, A. (2011). Mental models: An interdisciplinary synthesis of theory and methods. *Ecology and Society*, *16*(1), Article 46.

Kelly, L., Kerr, G., & Drennan, J. (2010). Avoidance of advertising in social networking sites. *Journal of Interactive Advertising*, *10*(2), 16–27.

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

Lapenta, G. H., & Jørgensen, R. F. (2015). Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday*, *20*(3). https://doi.org/10.5210/fm.v20i3.5568

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

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information, Communication & Society*, *21*(10), 1472–1492.

Norberg, P. A., Horne, D., & Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Ofcom. (2021). *Children and parents: Media use and attitudes report 2020/21*. https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2021

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

Pangrazio, L., & Selwyn, N. (2019). "Personal data literacies": A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, *21*(2), 419–437.

Podsakoff, P., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research. *Journal of Applied Psychology*, *88*(5), 879–903.

Robards, B., & Lincoln, S. (2019). Social media scroll back method. In P. Atkinson, S. Delamont, A. Cernat, J. W. Sakshaug, & R. A. Williams (Eds.), *SAGE research methods foundations* (1–10). SAGE.

Selwyn, N., & Pangrazio, L. (2018). Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data & Society*, *5*(1), 1–12.

Stoilova, M., Livingstone, S., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age*. London School of Economics.

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

Stoilova, M., Nandagiri, R., & Livingstone, S. (2019). Children's understanding of personal data and privacy online: A systematic evidence mapping. *Information, Communication & Society*, *24*(4), 557–575. https://doi.org/10.1080/1369118X.2019.1657164

Toff, B., & Nielsen, R. K. (2018). "I just Google it": Folk theories of distributed discovery. *Journal of Communication*, *68*(3), 636–657.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (Vol. 20, pp. 333–365). Springer.

van der Hof, S. (2017). I agree....Or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal*, *34*(2), 409–445.

van Reijmersdal, E. A., Rozendaal, E., Smink, N., van Noort, G., & Buijzen, M. (2017). Processes and effects of targeted online advertising among children. *International Journal of Advertising*, *36*(3), 396–414.

Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing*, *35*(1), 144–158.

Walrave, M., & Heirman, W. (2012). Adolescents, online marketing and privacy: Predicting adolescents' willingness to disclose personal information for marketing purposes. *Children & Society*, *27*, 434–447.

Walrave, M., Poels, K., Antheunis, M. L., Van den Broeck, E., & van Noort, G. (2016). Like or dislike? Adolescents' responses to personalized social network site advertising. *Journal of Marketing Communications*, *24*(6), 599–616.

Wash, R. (2010). Folk models of home computer security. *SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security*, *2010*(July), Article 11, 1–16. https://doi.org/10.1145/1837110.1837125

Yao, Y., Lo Re, D., & Wang, Y. (2017). Folk models of online behavioral advertising. In C. P. Lee & S. Poltrock (Eds.), *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 1957–1969). Association for Computing Machinery.

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., & Kim, S. (2019). Newsfeed native advertising on Facebook: Young millennials' knowledge, pet peeves, reactance and ad avoidance. *International Journal of Advertising*, *38*(5), 651–683.

Youn, S., & Shin, W. (2019). Teens' responses to Facebook newsfeed advertising: The effects of cognitive appraisal and social influence on privacy concerns and coping strategies. *Telematics and Informatics*, *38*, 30–45.

Zarouali, B., Poels, K., Ponnet, K., & Walrave, M. (2018). "Everything under control?": Privacy control salience influences both critical processing and perceived persuasiveness of targeted advertising among adolescents. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *12*(1). https://doi.org/10.5817/CP2018-1-5

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.

Zarouali, B., Verdoodt, V., Walrave, M., Poels, K., Ponnet, K., & Lievens, E. (2020). Adolescents' advertising literacy and privacy protection strategies in the context of targeted advertising on social networking sites: Implications for regulation. *Young Consumers*, *21*(3), 351–367.

About the Authors

Sanne Holvoet is a doctoral student at the Department of Communication Sciences at Ghent University. Her research focuses on teenagers' and teenager parents' engagement with online data collection in a commercial context and the subsequent personalized advertising.

Steffi De Jans is a postdoctoral researcher at the Department of Communication Sciences at Ghent University. She obtained her PhD in 2020 on how minors can be empowered to cope with digital advertising by examining different intervention tools to improve their advertising literacy. Now, she researches how consumers can be empowered to cope with digital advertising (such as social media advertising, influencer marketing) for dark consumption behavior (i.e., advertising for harmful products or behavior such as gambling and unhealthy eating behavior).

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

Liselot Hudders is associate professor at the Department of Communication Sciences at Ghent University. She conducts research on digital and responsible advertising with a focus on a minor audience.

Laura Herrewijn is a postdoctoral researcher at AP University of Applied Sciences and Arts Antwerp. Her research focuses on virtual environments (such as those represented in digital games and virtual/augmented reality apps) and their potential for the integration of persuasive communication (e.g., advertising, educational content, social content), along with consumer behavior (e.g., in-game purchases). In this context, she is interested in both effectiveness and ethical questions.