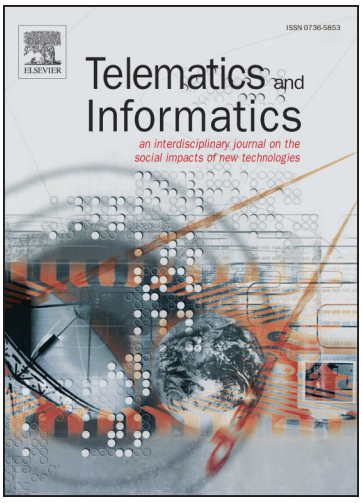
Journal Pre-proofs



Children's Perceptions of Fairness in a Data Disclosure Context: The Effect of a Reward on the Relationship between Privacy Literacy and Disclosure Behavior

Laurien Desimpelaere, Liselot Hudders, Dieneke Van de Sompel

PII: S0736-5853(21)00041-1
DOI: https://doi.org/10.1016/j.tele.2021.101602
Reference: TELE 101602

To appear in: *Telematics and Informatics*

Received Date: 2 October 2020
Revised Date: 26 February 2021
Accepted Date: 5 March 2021

Please cite this article as: Desimpelaere, L., Hudders, L., Van de Sompel, D., Children's Perceptions of Fairness in a Data Disclosure Context: The Effect of a Reward on the Relationship between Privacy Literacy and Disclosure Behavior, *Telematics and Informatics* (2021), doi: https://doi.org/10.1016/j.tele.2021.101602

Children's Perceptions of Fairness in a Data Disclosure Context: The Effect of a Reward on the Relationship between Privacy Literacy and Disclosure Behavior

Authors' names, affiliations and correspondence details:

Laurien Desimpelaere (corresponding author)
Ghent University, Faculty of Political and Social Sciences, Department of Communication Sciences, Belgium
Laurien.Desimpelaere@UGent.be
Korte Meer 7-9-11, 9000 Gent, Belgium
(0032) 9 264 68 66

Prof. Dr. Liselot Hudders
Ghent University, Faculty of Political and Social Sciences, Department of Communication Sciences, Ghent, Belgium
Ghent University, Faculty of Economics and Business Administration, Department of Marketing, Innovation and Organization
Liselot.Hudders@UGent.be
Korte Meer 7-9-11, 9000 Gent, Belgium
(0032) 9 264 91 89

Prof. Dr. Dieneke Van de Sompel
Ghent University, Faculty of Economics and Business Administration, Department of Marketing, Innovation and Organization
Ghent University, Faculty of Political and Social Sciences, Department of Communication Sciences, Ghent, Belgium
Dieneke.VandeSompel@UGent.be
Korte Meer 7-9-11, 9000 Gent, Belgium
(0032) 9 264 68 80

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 and online privacy.

Liselot Hudders is an assistant professor at the department of communication sciences at Ghent University and a postdoctoral fellow of the FWO at the marketing department. Her

research interests include persuasive communication, consumer behavior and advertising literacy.

Dieneke Van de Sompel is a visiting professor at the department of communication sciences at Ghent University. Her research interests include effects of advertising cues, persuasive communication and marketing on children's and adolescents' attitudes, behavior and motivations.

Funding

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).

Highlights

- Privacy literacy negatively influences disclosure behavior.
- Literate children find data practices more fair when a reward is provided.
- There is a positive relationship between perceived fairness and disclosure behavior.
- Older children engage more in privacy protective behavior.

Children's Perceptions of Fairness in a Data Disclosure Context: The Effect of a Reward on the Relationship between Privacy Literacy and Disclosure Behavior

Abstract

Children have increasingly become the target of commercial entities that seek their customer data. This study examines how young children deal with these requests and explores how enhancing their privacy literacy is related to real disclosure behavior. Additionally, the paper explores how this relationship is affected when companies provide a reward in exchange for the data and how it is mediated by how fair children think data practices are. An experiment with 496 children (9–13 years old) shows that privacy literacy negatively influences disclosure behavior. However, there is an interaction effect between privacy literacy and reward on perceived fairness, eventually affecting disclosure behavior. More specifically, children who are more literate find data practices to be fairer when a reward is provided, which in turn leads to greater data disclosure. Implications of the findings and directions for future research are discussed.

Keywords: online privacy; perceived fairness; privacy calculus; disclosure behavior; reward; young children

1 Introduction

As potential future consumers who have a great influence on the purchase decisions of their parents, children have become the target of commercial entities that seek their personal data for the creation of more personalized services, products, and advertising. A study on how developers collect and share personal data showed that two-thirds of apps played by preschool-aged children collected persistent digital identifiers (identification codes that can be traced back to the device's owner and that can be used for profiling and marketing purposes) and shared them with third-party marketing companies (Zhao et al., 2020).

In terms of regulation, more specifically under Europe's General Data Protection Regulation (GDPR), companies are not prohibited from using children's personal data for marketing purposes but should respect the imposed measures regarding data processing and protection when doing so (Information Commissioner's Office, 2018). Examples of such measures include providing comprehensible and concise information on how data will be processed and for what it will be used and having a lawful basis for data processing (e.g., consent) (Lievens and Verdoodt, 2018). When it comes to the latter, parental consent is needed for children below 16 years (in Belgium—the country where the current research was executed—this age barrier was lowered to 13 years) (Milkaite and Lievens, 2018).

Despite these additional measures, which should increase awareness about data processing, children struggle to understand the complexity of internet data and are not yet fully aware of the commercial use of their personal data (Livingstone et al., 2019). This can become even more problematic when businesses use creative methods to convince children to provide their personal data, hereby stressing the benefits of data disclosure. Examples can for instance be found in the provision of free products, access to online content, monetary incentives, contest participation, and customization benefits (Babula et al., 2017). This technique seems to be effective for teenagers, as Heirman et al. (2012) showed that six out of 10 teenagers (ages 12–18

years) disclosed their personal information in exchange for a commercial incentive, and Youn (2005) found that teenagers' (ages 14–18 years) intention to disclose gradually increased when they perceived more benefits from the website requesting their details.

Rewards may play a significant role in the so-called privacy calculus (Culnan and Armstrong, 1999; Laufer and Wolfe, 1977), that is, the assessment that people make when they are confronted with a disclosure request. This rationally based assessment concerns a trade-off between expected losses and potential gains stemming from disclosing their data. The extent to which they let this assessment rule in favor of or against disclosing depends on a number of factors. For example, individuals are more willing to share private information when risks can be compensated for with some kind of benefit (Li et al., 2010). These benefits are typically informational, commercial, economic, or social (Trepte et al., 2020). In particular, past research has shown that individuals are willing to disclose their personal information for benefits such as customization (Mothersbaugh et al., 2012) and monetary rewards (Shibchurn and Van, 2014). Besides the assessment of privacy costs and benefits related to data disclosure requests, individuals also make an implicit assessment of the exchange fairness. This is an individual's evaluation on how fair the information exchange is in terms of collection and subsequent use (Culnan and Armstrong, 1999). Malheiros et al. (2013) showed that consumers who perceived the data disclosure to be fairer disclosed more truthful data.

The concept of exchange fairness is also undoubtedly related to the aforementioned cost–benefit trade-off that comes with data disclosure requests. Individuals may for instance decide to not disclose their personal data when the requested data is unfair or when the purpose of data collection is unknown or irrelevant. The underlying assumption of both assessments (i.e., privacy calculus and exchange fairness) is the rational consideration that precedes the decision outcome (Kehr et al., 2015; Li et al., 2010). That is, individuals need to be aware of the privacy costs and gratifications when they are confronted with a data disclosure request

before they can actually form evaluations regarding its exchange fairness and decide on whether to disclose or not. Previous research has therefore suggested that literacy is important in privacy coping behavior (Trepte et al., 2015). The more consumers are aware of how their data can be used for commercial ends and how they can protect their online privacy, the more able they will be to put privacy protections into practice. Especially when it comes to young children, privacy literacy is often presented as a tool to empower them in the current digital environment and to help them manage their personal data online (De Wolf and Vanden Abeele, 2020).

While several factors (including both risk and benefit components) that influence disclosure behaviors have previously been identified, it is still unclear what the underlying mechanisms between antecedents and outcome behaviors are. For instance, there is a lack of insight into the predictive factor of literacy on perceived fairness and of fairness on disclosure behavior (Malheiros et al., 2013). Moreover, few studies have focused on the effects of the inclusion of rewards among children; those that did found that direct incentives increased children's disclosure intentions, and perceived benefits decreased privacy concerns (e.g., Heirman et al., 2012; Lwin et al., 2012; Walrave and Heirman, 2013; Youn, 2009). However, these studies took children's intentions into account rather than investigating how they actually acted upon a disclosure request. By measuring real disclosure behavior, the privacy paradox in which consumers' intentions contradict their real behavior can be ruled out (Kokolakis, 2017).

Considering both the need for more insights into the underlying mechanisms of privacy behavior and the call for more research on real disclosure behavior (see Baumeister et al., 2007), we aim to contribute to the existing theoretical foundation by investigating how moral reflection and, more precisely, perceived fairness act as potential mediators in the relationship between privacy literacy and information disclosure and how this relationship is affected by the provision of a reward. Investigating the impact of the benefit side of this trade-off on children's

disclosure behavior may provide valuable insights into children's decisions about privacy protection.

In this study, we focus on children between the ages of 9 and 13 years old. In addition to the increasing internet consumption among this age group, they also start to explore commercial websites online. Among the top 30 websites that British children accessed the most in May 2017, many commercial websites such as eBay and Amazon were noted (Ofcom, 2017). As commercial websites typically ask for personal data to facilitate the purchasing process, children may come into contact with commercial data disclosure requests at a young age. Also, from this age onwards they can begin to understand more complex and abstract concepts regarding privacy-related matters (Kumar et al., 2017), making it easier to address the topic of privacy when collecting research data. Children at this age also become capable of shifting between perspectives and understand that their point of view is not necessarily the same as that of others (John, 1999). This insight enables them to evaluate consumer-related matters on certain moral facets such as fairness and appropriateness (Wright et al., 2005; Zarouali et al., 2019). We believe policymakers may also benefit from the conclusions drawn from this study when developing guidelines on the provision of a reward in data disclosure contexts where young children are involved.

2 Literature Review

2.1 Theoretical framework

This study adopts the privacy calculus model as a theoretical framework to build on the hypotheses. The privacy calculus model (Laufer and Wolfe, 1977) is a common approach to analyze consumers' privacy perceptions and disclosure decisions. The theory of behavioral calculus originates from the idea that situational constraints are evaluated in view of potential outcomes in behavioral decision making. In the context of information disclosure, the theory proposes that when people decide on whether they want to disclose information, this calculus

is typically presented as a trade-off between the expected losses and potential gains that stem from disclosure. Previous studies (e.g. Kim et al., 2019) referred to these losses as risks and costs people relate to giving away their personal information. The gains are referred to as entailing benefits, such as rewards or social benefits, in return for their data.

Consumers' final behavior—either divulging personal data or refusing to do so—thus reflects the outcome of this cost–benefit trade-off. It is presumed that consumers only disclose personal data when potential benefits outweigh expected losses (Kokolakis, 2017). Previous studies have identified numerous factors that alter risk and benefit perceptions, such as the provision of monetary rewards (Li et al., 2010), personalized messages (Xu et al., 2011), sensitivity of the requested information (Mothersbaugh et al., 2012), and institutional trust and general privacy concerns (Kehr et al., 2015).

The privacy calculus theory sees the disclosure decision as a rather rational and conscious evaluation. Forming a cost–benefit trade-off is thus considered a true cognitive and rational process. This also implies that people actually need to be *aware* of the positive and negative consequences of data disclosure when evaluating these factors within a specific information disclosure context. This is not always the case, as people may not have good insights in the costs and benefits associated with data disclosure. Thus, the need for privacy literacy is an essential element and may also be viewed as an important antecedent for performing privacy calculus.

2.2 The Importance of Privacy Literacy

Privacy literacy has been proposed by many scholars as a key asset in effective privacy regulation and informed control of one's online identity (Trepte, Teutsch, Masur, Eichler, et al., 2015). More specifically, privacy literacy is related to the reluctance to provide personal data and the adoption of privacy protective behavior. For instance, in the context of social media, it was found that users with higher literacy changed their privacy settings on Facebook more

frequently (Bartsch and Dienlin, 2016). Weinberger et al. (2017) confirmed the link between literacy and coping behavior and stated that knowledge of ways and tools to enhance privacy protection (viz. passive privacy literacy) was positively related to the ability to effectively apply privacy-enhancing tools (viz. active privacy literacy). In other words, people who know how to protect their online privacy are also better at using effective measures to protect their privacy. Moreover, people who are privacy literate and are familiar with using privacy protective tools are also more likely to control the spread of their information than those with less knowledge (Park, 2013). A possible explanation for this can be found in people's different assessments of privacy risks when they are more literate. In particular, when consumers gain knowledge about how their information is used for marketing purposes, they may find it riskier to disclose their data or may perceive more privacy intrusion (Ham, 2017).

When it comes to children (ages 6–10 years), studies have shown that they can understand and identify certain types of privacy risks, such as stranger danger situations (Desimpelaere et al., 2020a) and information oversharing (Zhao et al., 2019). In the context of the so-called stranger danger situations (i.e., a form of danger that happens during the exchange of specific personal data in interpersonal communication), they are even able to employ a variety of privacy protective strategies such as refraining from providing any personal details and seeking parental guidance (Desimpelaere et al., 2020a). In commercial contexts, however, they have difficulties with identifying risks, such as online tracking (Zhao et al., 2019) and commercial data mining (Kumar et al., 2017).

In the analytical stage of consumer socialization, children (ages 7–11 years) begin to develop more complex consumer-related skills to function as consumers in the marketplace (John, 1999). However, they sometimes overvalue their ability to cope with privacy contexts and do not completely understand the risks of doing so. Thus, they can be more prone to marketers' attempts to convince consumers to divulge information (Shin et al., 2012).

One study that explored the effects of a privacy literacy training on children (ages 9–13 years) found that those children who watched a video on the collection and usage of personal data, and thus who gained more privacy literacy, disclosed less personal details than those who did not receive such training (Desimpelaere et al., 2020b). Likewise, it is important for children to have a certain level of privacy literacy as it helps them to make better disclosure decisions and to protect their privacy.

2.3 The Fairness of a Data Disclosure Request

The ability to make a moral judgement on the appropriateness of certain consumer-related affairs is an elementary aspect in making children well-informed and critical consumers (De Pauw et al., 2018; Friestad and Wright, 1994). Thus, if a person has attained a decent level of privacy literacy, it can be assumed that they are also able to reflect on whether a particular data disclosure request is fair or appropriate. This moral evaluation should also ideally become part of arriving at well-informed disclosure decisions.

Perceived fairness related to data requests represents individuals' beliefs that personal data will be collected and used as communicated by the data processor and that this happens in an ethical and fair way (Culnan and Armstrong, 1999). Drawing on the social contract theory, information exchange interactions between internet users and online businesses happen through social contracts (Donaldson and Dunfee, 1994). Such social contracts can be seen as a mutual agreement on the obligations or social norms for the involved parties (Li, 2012).

More specifically, people feel they have such a hypothetical contract when they share their personal data with online businesses. They put trust in the business to handle their data safely because according to the social contract, businesses are required to do so. When people feel that businesses correctly act upon the contract, and thus perceive the contract as more reliable, they will be more willing to provide personal data (Kruikemeier et al., 2020). If, for instance, the website collects data unrelated to the purpose of the information exchange, or

internet users encounter feelings of intrusiveness because their personal data are used unfairly, a breach of social contract is likely to be experienced (Li et al., 2010). As such, the reliability of the contract is questioned, and people may eventually decide not to share their personal information and instead safeguard their online privacy.

The fairness of information exchange is thus an important element in consumers' decisions on disclosure: the assessment of how fair the information exchange is can modify the outcome of the aforementioned privacy calculus or the cost–benefit trade-off (Li et al., 2010). That is, consumers may refrain from providing their personal data when they encounter feelings of unfairness (Sharma and Crossler, 2014). Children are also able to make moral judgements on consumer tactics. Kohlberg's (1984) moral stage theory proposes that moral thinking evolves from a focus on the self to a focus on the other and results from cognitive gains that come with age. In general, it is assumed that as children grow, their perspective-taking abilities are further developed, and they are able to judge actions by taking the other party's perspective, such as motives and intentions, into account. In particular, from the age of 7–8 years onwards, they develop cognitive skills such as a more complex theory of mind, that is, they are more skilled in understanding other people's points of view (Carpendale and Chandler, 1996). This is of great value for moral reasoning because evaluating commercial tactics on aspects like fairness and appropriateness typically involves understanding other people's motives (Zarouali et al., 2019).

In the context of advertising, the link between literacy and moral reflections is generally presented as a positive relationship. It is assumed that individuals become more skeptical and negative toward advertisements when they are more aware of persuasive attempts (Friestad and Wright, 1994). De Jans et al. (2019) showed that having knowledge is an important asset for being able to reflect critically on persuasive attempts. When people are aware of the different tactics and strategies that marketers use—in other words, when they have attained a certain

level of advertising literacy—it is easier for them to recognize and understand persuasive attempts. At the same time, this knowledge activates them to approach the ad more skeptically and to critically reflect on it because they understand the advertiser's motives to create such commercial content.

This relationship was demonstrated by a study that found that cognitive advertising literacy (related to knowledge) was correlated with moral advertising literacy (related to perceived fairness) among adolescents (ages 12–18 years) (De Jans et al., 2018). That is, the more insights adolescents have regarding the different tactics and strategies that marketers use, the less fair they think advertisements are. Another study that focused on children's (ages 9–11 years) perceptions on new advertising formats showed that when children were motivated to reflect on the tactics of unconscious persuasion, they formulated concerns regarding personalized advertising and perceived this to be a deceptive technique (De Pauw et al., 2018).

Therefore, we extend this line of thinking to the context of online privacy and expect that when children are more literate, they will find data practices less fair. This is because they will have a better view on the negative consequences that come with online data practices. In other words, they may have a broader and more nuanced view on the appropriateness of such practices, eventually leading them to formulate a more skeptical opinion on the use of personal data by commercial institutions.

H1: Children who are more (vs. less) privacy literate will perceive an online data disclosure request from a commercial company as less fair and will engage in less disclosure behavior.

2.4 The Moderating Role of a Reward

Consumers are often asked to provide their personal data in exchange for a reward or remuneration. Typical rewards entail access to media content, monetary incentives, personalized advertisements, and customization benefits (Babula et al., 2017; Li, 2012). The

privacy calculus model explains how these rewards are one part of the benefit and risk trade-off related to data disclosure. It posits that behavior is driven by utility maximization, whereby individuals aim at maximizing benefits and minimizing risks related to a certain behavior (Barth and de Jong, 2017). Consumers will thus only share their personal data when they perceive the benefits to be greater than the risks (Dinev and Hart, 2006). According to the reciprocity theory, "people respond to goodness with goodness and to unfavorable action with unfavorable action" (Mpinganjira and Maduku, 2019, p. 466). In other words, when businesses provide a reward, it can be expected that people will be more willing to disclose their personal data as they are motivated to respond favorably to positive actions.

In reality, a balance between privacy harms and opportunities often leads children to make decisions that favor immediate benefits of disclosure over pending privacy risks later on (Stoilova et al., 2019). Youn (2005), for instance, found that teenagers (ages 14–18 years) were more willing to provide personal data when they perceived adequate benefits. A possible reason for this is that at a young age, there is still an imbalance between children's cognitive control and their affective brain regions. This not yet fully matured cognitive control may thus be one reason for children's propensity towards arousing rewards (Defoe et al., 2015). Also, the extent to which disclosure advantages and disadvantages are portrayed by e-marketers may be yet another factor explaining the act of disclosing personal data. Advantages of disclosure requests are easier to recognize since e-marketers are clever to emphasize the benefits by, for instance, providing certain rewards in the form of content access or incentives. Recognizing risks in a disclosure context, in contrast, is much more difficult because it assumes that children have knowledge about the different risks related to the disclosure—which is usually not the case (Montgomery et al., 2017). Since privacy risks are often not explicitly stressed by data practitioners or can only be found when consulting the privacy notice, children—who lack

specific knowledge to correctly engage with these risks or inform themselves about the risks—may be more vulnerable.

Factors such as the presence of rewards and privacy risks may also influence consumers' perceptions of the fairness of the information exchange. Rewards tend to make data disclosure requests more attractive and eventually tempt consumers to engage in data disclosure, while privacy risks do the reverse (Premazzi et al., 2010). Put differently, the cost–benefit trade-off contributes to consumers' assessment of the fairness of the information exchange. This is where privacy literacy may play a crucial role. Children who are more literate may have a better notion of the positive and negative consequences of disclosure. When a reward is provided in exchange for personal data, literate children may find the disclosure request less fair as they may feel they are being "bribed" into giving their data and are more skeptical of such requests. In other words, they may find the disclosure request less fair because they know that their data will be used for commercial purposes, and they may feel deceived by the information receiver when a reward is promised. This leads us to the formulation of the following moderated mediation hypothesis (see Figure 1 for the conceptual model).

H2: When a commercial company includes a reward in an online data disclosure request (vs. no reward), children who are more literate will find the disclosure request less fair.

[Insert Figure 1 here]

3 Method

3.1 Design and Participants

A between-subjects experimental study design was used to test how children cope with a personal data request from a commercial company and to understand the effect of a reward on their disclosure behavior. The study was conducted in 10 primary schools in Flanders, Belgium. We obtained institutional ethical approval from the ethical review board of the university faculty as well as from the concerned primary schools. Children were only allowed to

participate after their parents provided written informed consent. In total, 496 children between 9 and 13 years old (M_{age} = 10.51, SD_{age} = .97) from the fourth (N = 184, 37%), fifth (N = 174, 35%), and sixth (N = 138, 28%) grade participated in the study. The sample was balanced across gender (N_{boys} = 255, 51%; N_{girls} = 241, 49%).

3.2 Stimuli and Pretest

For the actual study, a mock-up game website was constructed, which exposed children to a data disclosure request. As the aim was to create a website that looked as realistic as possible, the game website originated from a real existing and popular soda brand because its products are extensively consumed and well-known among young children. Before playing the advergame, children in this study were confronted with a data request from this commercial brand ("Provide your details quickly!"), where they could decide to disclose their personal details or not. Half of them got to see the reward condition in this stage, whereas in the control condition, this disclosure was not displayed.

The website consisted of three pages. On the introduction page, to manipulate the provision of a reward (versus lack of reward), we either mentioned children could win a theme park ticket in return for their personal data or did not include such a statement (see Figure 2). For purposes of realism, we included a statement that made this data request comply with today's regulations on transparency of data usage (i.e., GDPR), namely that the brand would use personal data for advertising purposes and share these data with third parties.

[Insert Figure 2 here]

On the second page (Figure 3a), children were asked for six types of personal details (e.g., age and name) with an option to not give any data (by means of a "I don't want to share my personal details" button) before being able to move onto the actual game page. The number of personal details given on this page enabled us to calculate a score reflecting the real disclosure behavior (see Section 3.4).

On the third page, the actual game was displayed. Children were instructed to catch as many bottles as possible in 1 minute (Figure 3b).

[Insert Figure 3 here]

In order to decide on the ideal reward, a within-subjects pretest was conducted among 97 children ages 8–11 years (M = 9.79, SD = .88; 40% female). Children were asked to envision browsing the website of a popular soda brand to play a game. Then they were asked to rate to what extent they liked different rewards that the brand would provide in exchange for their personal data. These rewards included a movie ticket, a tennis racket, a theme park ticket, and a comic strip (all were chosen because of their gender and age neutrality). Children were then asked to indicate how much they liked and valued each reward.

Paired samples t-tests revealed that the movie ticket and the theme park ticket had the highest mean values for reward liking and value (see Table 1). There was no statistical difference between the extent to which children liked the two rewards ($t(96) = -.39$, $p = .697$). Children did value the theme park ticket more than the movie ticket ($t(96) = -2.15$, $p = .034$). Based on the results, we decided to include the theme park ticket as the hypothetical reward in our study.

[Insert Table 1 here]

To manipulate privacy literacy, half of the children received privacy literacy training in the form of an educational video. We chose to show a privacy literacy training video to some children based on the following assumptions: that children would initially have a rather low privacy literacy and that there would be low variation in the literacy levels for the age group participating in this study. However, Desimpelaere et al. (2020b) showed that children act differently upon disclosure requests when they are more aware of the consequences related to data sharing (viz. they disclose less details when they are more literate). Therefore, we deemed having different levels of privacy literacy was necessary for this study. As earlier studies

demonstrated that privacy education is effective at raising children's privacy knowledge (e.g. Zhang-Kennedy et al., 2017), we exposed half of the children to privacy literacy training in the form of an educational video. The other half of the children received no training, but for reasons of uniformity, they watched a video on an unrelated topic. We believed that the mix of children having watched a privacy literacy video and children not having watched such training would enable us to have more variation in children's knowledge levels. We thus used children's privacy literacy as a continuous independent variable in our analyses.

The training videos were developed and pretested in another study (Desimpelaere et al., 2020b; see Figure 4 for screenshots of the privacy literacy training and control video). The basic principles of personal data collection and usage as well as the consequences related to consumer data disclosure were explained in the privacy literacy training video. The video also emphasized the importance of data protection and proposed several strategies to cope with data disclosure requests, including asking for parental guidance, reading privacy statements, refusing to provide personal data, and sharing only fictive details. Children who were allocated to the control group watched a video that explained the consequences of global warming and the actions that people can take to slow this process. The results of this study showed that the privacy literacy training enhanced children's privacy literacy (vs. the control video). We therefore argue that the initial goal for obtaining different levels of privacy literacy was achieved, and we consequently used the variable (level of) privacy literacy (and not the presence or absence of the privacy literacy training itself) in the following results (see Figure 5 for the distribution of the score on privacy literacy).

[Insert Figures 4 and 5 here]

3.3 Procedure

This study began by shortly briefing the children about the research's procedure. Children then watched either the privacy literacy training video or the control video. This

happened at the class level, meaning that all children from the same class watched the same video. Children could then play three online games, the first two of which were included to cover up the true purpose of the experiment (Bubbleshooter and Slither.io, two games that are freely available on the internet). Children played both games for approximately 3 minutes before moving to the self-constructed game website containing the reward manipulations, where they responded to the data request. Finally, children were forwarded to the self-reported survey. The researcher read out loud each question for all children in the classroom (to control for differences in reading ability), after which the children answered the question (they could only continue to the next question when everybody in the classroom had answered a particular question).

3.4 Measures

After exposing children to a data disclosure request, they moved onto the questionnaire, which included measures for privacy literacy, perceived advantage, perceived fairness, real disclosure behavior, and socio-demographic variables. To assess children's online privacy literacy, six true/false items were used, four of which came from the scale by Kezer et al. (2016) (e.g., "It is a good idea to provide your personal details, even if you do not entirely know what they will do with them") and two of which were self-composed (e.g., "Cookies are little programs that are installed on your computer and save information on which websites you visit"). The number of correct answers provided by the child was summated (M = 3.68, SD = 1.26).

For reasons of time constraints and to avoid respondent fatigue, the measurement of perceived fairness and advantage was done with a single item each. Research shows that constructs in marketing studies consisting of a concrete singular object and a concrete attribute are not necessarily inferior to the quality of multiple-item constructs (Bergkvist and Rossiter, 2007). Another study among ninth grade students showed that single-scale measures were

similar to corresponding longer scales (Gogol et al., 2014). In several domains, single-item measures have also been proven to be effective and valid when working with minors (Sattler et al., 2017), as they are much shorter and simpler to present to this age group.

Perceived fairness was assessed based on the single-item measure that Chatterjee and McGinnis (2010) and Campbell (1999) used in their studies: "How fair do you think it is that this brand asks for and uses your personal data?" (1 = not at all fair, 5 = very fair; M = 2.26, SD = 1.08). To assess if children perceived the reward and no-reward condition correctly, a single-item manipulation check assessed if children perceived advantages while being exposed to the site (1 = not at all, 5 = a lot; M = 2.42, SD = 1.04).

To assess children's disclosure behavior, we used the same approach as Metzger (2007). As mentioned before, the website asked children about six personal details, which children could fill out (with authentic or fake information) or could leave blank. In the questionnaire, children saw these entries again and needed to indicate for each data entry record they filled out (viz. first name, last name, gender, age, street name, postal code) whether it was (in)correct. This led us determine whether children had lied when entering their details. By explicitly mentioning that we did not want them to adapt incorrect details but that we only wanted to know what information was wrong or correct, we intended to avoid socially desirable answers. The number of accurately provided private details was then summated. A score of 0 was assigned to children who clicked on the "I don't want to share my personal details" button (indicating they did not want to share their data) or to children who lied about all requested details. The higher the score, the more correct details were shared, thus reflecting less engagement in privacy protective behavior (range: 0–6, M = 2.19, SD = 1.28). Finally, participants also completed questions on socio-demographics (viz. gender, age, grade, school).

4 Results

4.1 Control Measures and Randomization

Manipulation controls were performed via independent *t*-tests and showed that the privacy literacy training had a positive effect on privacy literacy ($t(494) = -9.81$, $p < .001$, $d = .88$). Children who saw the privacy literacy training video ($M = 4.20$, $SD = 1.13$) were more literate than children who watched the control video ($M = 3.19$, $SD = 1.19$). Our previously stated aim to have different levels of privacy literacy was thus achieved, and we thus continued to use the level of privacy literacy as an independent variable in the following analyses to test the proposed hypotheses. Second, the reward condition was also manipulated successfully. Those who were exposed to a reward ($M = 2.52$, $SD = 1.04$) perceived more benefits than those who were not exposed to such reward ($M = 2.28$, $SD = 1.03$; $t(494) = -2.51$, $p = .012$, $d = .23$).

There were no gender ($\chi^2(1) = .036$, $p = .851$) or age ($t(476.67) = 1.53$, $p = .126$) differences between the reward condition and the control group. For privacy literacy, there were no differences between boys' and girls' level of literacy ($t(494) = -.91$, $p = .386$), but a simple linear regression showed that age did significantly predict privacy literacy ($F(1, 495) = 4.52$, $p = .034$, $R^2 = .009$). Therefore, we decided to include age as a covariate in our analyses.

4.2 Correlations

Before testing the hypotheses, we examined how the different constructs were related (see Table 2). Privacy literacy was negatively correlated with disclosure behavior. That is, the higher the child's privacy literacy was, the less accurate personal details were given. Perceived fairness was positively correlated with perceived advantage and disclosure behavior. In other words, the fairer the data disclosure request was perceived to be, the more advantages and accurate details were provided. Perceived advantage was also positively correlated with disclosure behavior, meaning that the more advantages were experienced, the more accurate details were provided.

[Insert Table 2 here]

4.3 The Mediating Role of Perceived Fairness on the Relationship between Privacy Literacy and Disclosure Behavior

For the first hypothesis, a mediation analysis was conducted to investigate the relationship between privacy literacy and disclosure behavior through perceived fairness (Hayes, 2018; PROCESS, model 4, 5000 bootstraps; see Table 3). Age was included as a covariate in this analysis. There was a direct negative effect of privacy literacy on disclosure behavior (B = –.36, SE = .09, p < .001). Children who were more literate engaged more in privacy protective behavior such as disclosing untruthful details or refusing to provide data. No direct effect was found between privacy literacy and perceived fairness (B = .04, SE = .04, p = .289), nor did perceived fairness mediate the relationship between privacy literacy and disclosure behavior, disconfirming H1 (B = .02, SE = .02, 95% CI [–.0179, .0611]). There was, however, a positive effect of perceived fairness on disclosure behavior (B = .46, SE = .11, p < .001), meaning that when children perceived the data disclosure request as fairer, the more truthful personal details they provided.

[Insert Table 3 here]

The covariate age did not affect perceived fairness (B = –.06, SE = .05, p = .233) but did influence disclosure behavior (B = –.24, SE = .12, p = .046). The older children were, the less truthful details they disclosed.

4.4 The Moderating Role of a Reward on the Relationship between Privacy Literacy and Disclosure Behavior

In order to investigate the moderating effect of a reward on the relationship between privacy literacy and disclosure behavior as mediated by perceived fairness (H2), a moderated mediation analysis was conducted (Hayes, 2018; PROCESS, model 7, 5000 bootstraps; see Figure 6). Again, age was included as a covariate.

[Insert Figure 6 here]

There was an indirect effect of privacy literacy (x) on disclosure behavior (y) through perceived fairness (m), depending on the reward condition (w) (*B* = .08, *SE* = .04, 95% CI [.0101, .1853]; see Table 4).

[Insert Table 4 here]

More specifically, when a reward was given, there was a positive effect of literacy on disclosure behavior, mediated through perceived fairness (*B* = .06, *SE* = .03, 95% CI [.0078, .1185]). For the condition in which a reward was provided, a higher level of privacy literacy led children to perceive the data disclosure request to be *fairer* (see Figure 7), and this eventually convinced them to engage in *greater* data disclosure. However, this is the exact opposite of what H2 proposes, and thus we could not accept H2. For the condition in which no reward was provided, there was no significant relationship between children's privacy literacy and perceived fairness (*B*= –.03, *SE* = .03, 95% CI [–.0970, .0275]).

[Insert Figure 7 here]

There was also a negative main effect for the provision of a reward on perceived fairness (*B* = –.61, *SE* = .30, *p* = .043). Thus, when a reward was provided, children perceived the data exchange request to be less fair, and this eventually led to less disclosure. Regarding the covariate age, we found no significant effect of this variable on perceived fairness (*B* = –.05, *SE* = .05, *p* = .284), but there was again a negative effect of age on disclosure behavior (*B* = –.24, *SE* = .12, *p* = .046).

5 Discussion

Following previous calls for more research on children's real privacy behavior (Baumeister et al., 2007; Montgomery et al., 2017), this study investigated how children's privacy literacy influences real disclosure behavior and how it is mediated by perceived fairness and moderated by the provision of a reward. Several conclusions can be derived from this study.

Privacy literacy plays an important role in the extent to which children protect their online privacy. Our results showed that when children are more literate about the use of their personal data for commercial purposes, such as personalized advertisements, they disclose less truthful details by either lying about their personal information or refusing to provide them in the first place. This is in line with earlier research (Desimpelaere et al., 2020b) that showed that privacy literacy training enhanced the adaptation of privacy protective behavior.

The relationship between literacy and behavior, however, changes completely when a reward is introduced to the scenario. In opposition to our initial expectation, we found that when a reward was provided, children with higher literacy experienced the data disclosure request to be fairer than those who had lower levels of such knowledge, eventually leading to a higher number of disclosed truthful items. A number of explanations can underlie this effect. First, children could possibly have a better understanding of the consequences of data practices when they are more literate. Following the privacy calculus theory (Culnan and Armstrong, 1999), privacy literacy enables rationality toward a cost–benefit trade-off, meaning that children who are more aware of the negative consequences are less likely to divulge personal data. In other words, the risks outbalanced the benefits (which is also supported by our finding that the more privacy literate children were, the less details they provided). Thus, the privacy calculus model sees consumers as rational agents able to balance advantages and disadvantages against each other before making a decision on disclosure requests (Kokolakis, 2017), and hence, literacy can ease the assessment of this trade-off. However, situational cues such as immediate rewards may alleviate potential risks and may override rational privacy-related thinking (Barth and de Jong, 2017). In this sense, the fairness heuristic theory (Lind et al., 2001) stipulates that people rely on fairness cues to identify fair parties and to determine whether they are being treated correctly. It may thus be that a reward functions as a fairness cue that guides children to make decisions on data disclosure. In this sense, more literate children may thus look for specific

fairness cues in a disclosure context, hereby attempting to compensate for the risks that are involved with such disclosure. As a result, they may value a reward much more because they may perceive the incentive as part of a fair information exchange whereby both parties exchange some good.

Second, it may also be that the more insight children have into the risks related to data disclosure, the less severe the risks are perceived to be. As previous research suggests, children are often warned about stranger danger situations in which malicious individuals misuse children's data (Zhang-Kennedy et al., 2016). However, when children become more aware of the consequences of data disclosure in *commercial* contexts, they may perceive data disclosure in these contexts to be safer. In this sense, a reward may actually encourage them to disclose details even more.

Third, the effects may also be explained by children's higher confidence in their ability to deal with data disclosure requests that results from being more literate. Confidence that arises from such knowledge may weaken their resistance to the presence of rewards in an online disclosure situation. In the context of advertising, it was also found that knowledge does not always compensate for the influence of persuasive messages. For instance, Youn and Shin (2020) found that adolescents with a high persuasion knowledge (viz. the ability to recognize and understand advertisers' persuasive motives and tactics of commercial messages; Friestad and Wright (1994)) found the advertisement more relevant and, at the same time, experienced less feelings of privacy infringement.

It thus seems that privacy literacy, and perhaps the confidence stemming from this enhanced knowledge, is in fact a hurdle for critical assessment when a reward is traded for personal data. Thus, in contrast to what the privacy calculus theory suggests, consumers, and more specifically, children, are not always rational agents who deliberately weigh benefits against risks. Even though they are literate, the decision to disclose is also dependent on

situation-specific cues. In this sense, rewards can eventually lead users to favor instant gratification at the cost of future risks and makes them more willing to share personal information (Waldman, 2020).

Besides the effects of privacy literacy on disclosure behavior, the extent to which children find a disclosure request to be fair is also an important element in the decision-making process for data disclosure. More specifically, when children find the disclosure request to be fair, they disclose more truthful details and thus engage less in privacy protective behavior. The relationship between moral reflection and behavior was also acknowledged in a study on adolescents' (ages 12–18 years) advertising literacy (De Jans et al., 2018). In that study, it was found that adolescents who were more skeptical toward advertisements engaged more in advertising resistance, such as avoiding seeing the advertisements. Thus, the moral reflection on certain consumer practices, such as perceiving something as unfair or being skeptical, may play a crucial role in accepting or rejecting consumer practices.

Finally, in addition to the level of privacy literacy, age seems to play an important role in children's assessments on data disclosure. In line with previous research (Desimpelaere et al., 2020b), this study showed that the older children were, the less truthful details they disclosed. A potential reason for this finding is that when children become older, they gain more familiarity with internet hazards. In turn, internet users who are more experienced tend to adopt more [illegible] (Milne et al., 2004).

6 Implications

In light of this study's findings, a few implications for e-practitioners, researchers, and policymakers can be derived. If we want children to make well-informed decisions on data disclosure, the acquirement of privacy literacy is key, as this study has demonstrated. Therefore, the first implication aligns with previous research calls that stress the importance of privacy literacy and education (Trepte, Teutsch, Masur, Eicher, et al., 2015). Cognitive skills (viz.

knowing how e-practitioners collect and use personal data for commercial purposes) seem to be effective for reducing the amount of data provided voluntarily. Increasing children's literacy on this topic can be done in a number of ways, for example, by focusing on educational programs that can be taught in school environments and via national media (e.g., publicly funded television stations with a channel for children that broadcast educational and informational content).

One of the findings also showed that children's literacy gradually develops over the years. However, in the context of advertising, research has shown that children ages 12 and under have not yet reached an adult-like level of advertising literacy (Rozendaal et al., 2010). It is thus rather questionable that the necessary level of privacy literacy is fully developed by the age of 13 (the age range in this study was between 9 and 13 years). Therefore, it is important to teach children from a young age to critically reflect on data collection practices, and, by extension, general consumer practices so that they are able to develop these skills throughout childhood.

Also, this study showed that the extent to which a data request is perceived as fair affects the decision outcome on disclosure. Thus, content wise, these educational efforts should also pay attention to when data practices are appropriate and fair and should ideally teach children to reflect critically on data requests and judge them on their appropriateness. In this way, education leads to children not only being able to recognize situations in which their data are collected and used for commercial aims but also to formulate opinions on how appropriate or fair the concerned practice is. Moreover, governments should focus on national information campaigns that go beyond the typical stranger danger situations in interpersonal communication (Desimpelaere et al., 2020a) and incorporate negative consequences of data practices in other (e.g., commercial) contexts as well.

Commercial platforms should also make affordances. For instance, they could do so by informing users about the tactics used and consequences of data disclosures when a data disclosure request is prompted. At the very least, there needs to be a clear and easy-to-understand disclosure. One prescriptive form of standard disclosure ideally signals the consumer (or the child) that their data will be collected and used (Campbell and Grimm, 2019).

Our study also showed that a high level of privacy literacy can actually be an obstacle to effective privacy management in instances where a reward is provided. That certainly does not mean that children should not be educated in order to attenuate these effects, but instead, e-practitioners should be prohibited from distributing explicit rewards in return for personal data, especially when it comes to young children. Thus, the industry could benefit from clearer information on the implementation of the current legislation. This information could be distributed through information sessions or by sharing best practices.

Finally, we wonder whether the current legislation goes far enough in protecting children's online privacy. General regulation and self-regulatory initiatives by the (advertising) industry itself could consider completely banning companies from gathering children's data in the first place rather than setting limitations or barriers (e.g., verifiable parental consent) for the collection and processing of their data (Vermeulen and Lievens, 2017). We believe that the combination of educating children, setting restrictions, and sharing guidelines on dealing with children's personal data would eventually result in more empowered kids who are able to understand and respond to data requests responsibly.

7 Limitations and Directions for Future Research

In this section, several limitations are addressed that may serve as suggestions for further research. First, to obtain different levels of privacy literacy, we used a privacy literacy training video to enhance the children's literacy. Little time elapsed between showing the privacy literacy video and the actual experiment. This could imply that the effects of the video were

still very salient while children participated in the experiment, which is not entirely realistic in a real-life setting. Future research should consider investigating whether long-term effects can be detected when the period between exposure and the actual experiment is prolonged, and also whether the found effects hold when no such educational intervention is used.

Next, we want to point out that no prior test was done to assess any existing differences in privacy literacy between the two groups (those who watched the privacy literacy training and those who were in the control group). Although we believe such pretests could have influenced participants in such a way that it affected their privacy perceptions and disclosure behavior later in the study, the found results could have benefit from controlling for existing literacy differences (e.g., performing a pretest a few days before the experiment).

There are also a few limitations to be noted with respect to the stimuli materials used. First, the results cannot be generalized due to the type of reward used in this study. Companies use a number of tempting benefits other than chances to win theme park tickets. Future studies could therefore explore different types of benefits, such as access to games, provisions of more tangible assets (books, toys, etc.), and more (Babula et al., 2017).

Also, we recognize that the current type of reward (i.e., theme park ticket) is extremely attractive for the target group in this study. Future studies should consider less attractive incentives as well (e.g., access to the game itself or chances to win a brand product) in order to further unravel the found interaction effect.

Second, in order to create a realistic website, an existing brand was used which is familiar and well-known among children. Its strong reputation might have led children to respond more favorably to data requests compared to less reputable brands, as suggested by the reciprocity theory. As such, the reputation of a company as being an ethical or unethical brand might strongly affect how people respond to data requests from that company (Mpinganjira and

Maduku, 2019). It would therefore be interesting to examine how children respond to data requests from a company with a less strong or even with an unethical brand reputation.

Third, as previously mentioned, the GDPR states that institutions should ask for parental consent when processing data belonging to children under 16 years of age. Due to practical constraints, we could not involve parents in the children's disclosure decision in this experiment. However, in reality, children may make completely different decisions when they need to ask their parents' permission first. However, we opine that it is difficult to incorporate parents into such an experiment, and we also question whether children actually do always ask for their parents' permission in reality. We suggest that the results should be interpreted with this limitation in mind.

The final limitation regarding the stimuli is related to the different types of personal information (viz. first and last name, gender, age, street name, and postal code) that were requested. In a real-life setting, asking for a user's address is often only done when it concerns an online purchase process and not for simple sign-up occasions. We did this deliberately to ensure variation possibilities in the extent to which children perceived the request as severe. However, this could affect the practical applicability of the results.

We also want to elaborate on the single-item measures used in this study. Despite the advantages that single-item measures may have when performing research with children (e.g., short, less time consuming, easy to understand, and valid), future research may consider include multi-item measures if there is time to do so. This way, the internal validity of the concerned scale can be better guaranteed.

We also agree with De Pauw et al. (2018) suggestion to incorporate questions in future research that uncover the rationale behind children's judgements on the (in)appropriateness of the concerned data practices and the used tactics. Besides asking them how fair a particular data disclosure request is, it may be more valuable to let them explain the process of their judgement

(why?). This way, children learn to critically reflect on the appropriateness (taking into account the pros and cons) when they are confronted with such requests, and these insights may eventually be valuable for the development of privacy educational programs.

References

Babula, E., Mrzygłód, U., Poszewiecki, A., 2017. Consumers' need of privacy protection: Experimental results. Econ. Sociol. 10(2), 74–86. doi:10.14254/2071-789X.2017/10-2/6

Barth, S., de Jong, M.D.T., 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior: A systematic literature review. Telemat. Inform. 34(7), 1038–1058. doi:10.1016/j.tele.2017.04.013

Bartsch, M., Dienlin, T., 2016. Control your Facebook: An analysis of online privacy literacy. Comput. Human Behav. 56, 147–154. doi:10.1016/j.chb.2015.11.022

Baumeister, R.F., Vohs, K.D., Funder, D.C., 2007. Psychology as the science of self-reports and finger movements: Whatever happened to actual behavior? Perspect. Psychol. Sci. 2(4), 396–403. doi:10.1111/j.1745-6916.2007.00051.x.

Bergkvist, L., Rossiter, J.R., 2007. The predictive validity of multiple-item versus single-item measures of the same constructs. J. Mark. Res. 44(2), 175–184. doi:10.1509/jmkr.44.2.175

Campbell, C., Grimm, P.E., 2019. The challenges native advertising poses: Exploring potential federal trade commission responses and identifying research needs. J. Public Policy Mark. 38(1), 110–123. doi:10.1177/0743915618818576

Campbell, M.C., 1999. Perceptions of price unfairness: Antecedents and consequences. J. Mark. Res. 36(2), 187–199. doi:10.1177/002224379903600204

Carpendale, J. I., & Chandler, M. J. (1996). On the distinction between false belief understanding and subscribing to an interpretive theory of mind. Child development, 67(4), 1686–1706. doi:10.2307/1131725

Chatterjee, P., McGinnis, J., 2010. Customized online promotions: Moderating effect of promotion type on deal value, perceived fairness, and purchase intent. J. Appl. Bus. Res. 26(4), 13–20. doi:10.19030/jabr.v26i4.302

Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organ. Sci. 10(1), 104–115. doi:10.1287/orsc.10.1.104

De Jans, S., Hudders, L., Cauberghe, V., 2018. Adolescents' self-reported level of dispositional advertising literacy: How do adolescents resist advertising in the current commercial media environment? Young Consum. 19(4), 402–420. doi:10.1108/YC-02-2018-00782

De Jans, S., Hudders, L., Herrewijn, L., Van Geit, K., & Cauberghe, V. (2019). Serious games going beyond the Call of Duty: Impact of an advertising literacy mini-game platform on adolescents' motivational outcomes through user experiences and learning outcomes. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13(2), article 3. doi:10.5817/CP2019-2-3

De Pauw, P., De Wolf, R., Hudders, L., Cauberghe, V., 2018. From persuasive messages to tactics: Exploring children's knowledge and judgement of new advertising formats. New Media Soc. 20(7), 2604–2628. doi:10.1177/1461444817728425

De Wolf, R., Vanden Abeele, M.M., 2020. Children's voices on privacy management and data responsibilization. Media Commun. 8(4), 158–162. doi:10.17645/mac.v8i4.3722

Defoe, I.N., Dubas, J.S., Figner, B., van Aken, M.A., 2015. A meta-analysis on age differences in risky decision making: Adolescents versus children and adults. Psychol. Bull. 141, 48–84. doi:10.1037/a0038088

Desimpelaere, L., Hudders, L., Van de Sompel, D., 2020a. Children's and parents' perceptions of online commercial data practices: A qualitative study. Media Commun. 8(4), 163–174. doi:10.17645/mac.v8i4.3232

Desimpelaere, L., Hudders, L., Van de Sompel, D., 2020b. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. Comput Human Behav. 110. doi:10.1016/j.chb.2020.106382

Dinev, T., Hart, P. 2006. An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. 17(1), 61-80. doi:10.1287/isre.1060.0080

Donaldson, T., Dunfee, T.W., 1994. Toward a unified conception of business ethics: Integrative social contracts theory. Acad. Manag. Rev. 19(2), 252–284. doi:10.5465/amr.1994.9410210749

Friestad, M., Wright, P., 1994. The persuasion knowledge model: How people cope with persuasion attempts. J. Consum. Res. 21(1), 1–31. doi:10.1086/209380

Gogol, K., Brunner, M., Goetz, T., Martin, R., Ugen, S., Keller, U., Fischbach, A., Preckel, F., 2014. "My questionnaire is too long!" The assessments of motivational-affective constructs with three-item and single-item measures. Contemp. Educ. Psychol. 39(3), 188–205. doi:10.1016/j.cedpsych.2014.04.002

Ham, C.-D., 2017. Exploring how consumers cope with online behavioral advertising. Int. J. Advert. 36(4), 632–658. doi:10.1080/02650487.2016.1239878

Hayes, A. F. 2018. Introduction to mediation, moderation, and conditional process analysis: A regression-based approach. Guilford publications (2nd edition).

Heirman, W., Walrave, M., Ponnet, K., 2012. Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. Cyberpsychology Behav. Soc. Netw. 16(2), 81–87. doi:10.1089/cyber.2012.0041

John, D., 1999. Consumer socialization of children: A retrospective look at twenty-five years of research. J. Consum. Res. 26(3), 183–213. doi:10.1086/209559

Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inf. Syst. J. 25, 607–635. doi:10.1111/isj.12062

Kezer, M., Sevi, B., Cemalcilar, Z., Baruh, L. 2016. Age differences in privacy attitudes, literacy and privacy management on Facebook. Cyberpsychol.: J. Psychosoc. Res. Cyberspace, 10(1). doi:10.5817/CP2016-1-2

Kim, D., Park, K., Park, Y., Ahn, J.-H., 2019. Willingness to provide personal information: Perspective of privacy calculus in IoT services. Comput. Human Behav. 92, 273–281. doi:10.1016/j.chb.2018.11.022

Kohlberg, L., Ricks, D., Snarey, J. 1984. Childhood development as a predictor of adaptation in adulthood. Genet. Psychol. Monogr. 110(1), 91−172.

Kokolakis, S., 2017. Privacy attitudes and privacy behavior. Comput. Secur. 64(C), 122–134. doi:10.1016/j.cose.2015.07.002

Kruikemeier, S., Boerman, S. C., Bol, N., 2020. Breaching the contract? Using social contract theory to explain individuals' online behavior to safeguard privacy. Media Psychol. 23, 269–292. doi:10.1080/15213269.2019.1598434

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. Proc. ACM Human-Comput. Interact. 1(CSCW), 64. doi:10.1145/3134699

Laufer, R.S., Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. J. Soc. Issues 33(3), 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x

Li, H., Sarathy, R., Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. J. Comput. Inf. Syst. 51(1), 62–71.

Li, Y., 2012. Theories in online information privacy research: A critical review and an integrated framework. Decis. Support Syst. 54(1), 471–481. doi:10.1016/j.dss.2012.06.010

Lievens, E., Verdoodt, V., 2018. Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. Comput. Law Secur. Rev. 34(2), 269–278. doi:10.1016/j.clsr.2017.09.007

Lind, E., Kray, L., Thompson, L., 2001. Primacy effects in justice judgments: Testing predictions from fairness heuristic theory. Organ. Behav. Human Decis. Process. 85, 189–210. doi:10.1006/obhd.2000.2937

Livingstone, S., Stoilova, M., Nandagiri, R., 2019. Children's data and privacy online: Growing up in a digital age: An evidence review. London: London School of Economics and Political Science.

Lwin, M.O., Miyazaki, A.D., Stanaland, A.J., Lee, E., 2012. Online usage motive and information disclosure for preteen children. Young Consum. 13(4), 345–356. doi:10.1108/17473611211282590

Malheiros, M., Preibusch, S., Sasse, M.A., 2013. "Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. Paper presented at the International Conference on Trust and Trustworthy Computing.

Metzger, M.J. 2007. Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. J. Am. Soc. Inf. Sci. Technol. 58(13), 2078–2091.

Milkaite, I., Lievens, E., 2018. Counting down to 25 May 2018: Mapping the GDPR age of consent across the EU. Better Internet Kids.

Milne, G.R., Rohm, A.J., Bahl, S., 2004. Consumers' protection of online privacy and identity. J. Consum. Aff. 38(2), 217–232. doi:10.1111/j.1745-6606.2004.tb00865.x

Montgomery, K.C., Chester, J., Milosevic, T., 2017. Children's privacy in the big data era: Research opportunities. Pediatr. 140(Supplement 2), S117–S121. doi:10.1542/peds.2016-1758O

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E., Wang, S., 2012. Disclosure antecedents in an online service context: The role of sensitivity of information. J. Serv. Res. 15(1), 76–98. doi:10.1177/1094670511424924

Mpinganjira, M., Maduku, D.K., 2019. Ethics of mobile behavioral advertising: Antecedents and outcomes of perceived ethical value of advertised brands. J. Bus. Res. 95, 464–478. doi:10.1016/j.jbusres.2018.07.037

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

Park, Y.J., 2013. Digital literacy and privacy behavior online. Commun. Res. 40(2), 215–236. doi:10.1177/0093650211418338

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., Hofacker, C.F., 2010. Customer information sharing with e-vendors: The roles of incentives and trust. Int. J. Electron. Commer. 14(3), 63–91. doi:10.2753/JEC1086-4415140304

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

Sattler, A.F., Tiede, M.S., Dammann, J.E., Jensen, A.H., Walton, G.A., Whiteside, S.P. 2017. Utility of a single-item child anxiety rating for use in community practice. Prof. Psychol.: Res. Pract. 48(4), 259–266. doi:10.1037/pro0000096

Sharma, S., Crossler, R.E., 2014. Disclosing too much? Situational factors affecting information disclosure in social commerce environment. Electron. Commer. Res. Appl. 13, 305–319. doi:10.1016/j.elerap.2014.06.007

Shibchurn, J., Van, X.B., 2014. Investigating effects of monetary reward on information disclosure by online social networks users. Paper presented at the 47th Hawaii International Conference on System Sciences (HICSS), 2014.

Shin, W., Huh, J., Faber, R., 2012. Tweens' online privacy risks and the role of parental mediation. J. Broadcast. Electron. Media 56(4), 632–649. doi:10.1080/08838151.2012.732135

Stoilova, M., Nandagiri, R., Livingstone, S., 2019. Children's understanding of personal data and privacy online–A systematic evidence mapping. Inform. Commun. Soc., 1-19. doi:10.1080/1369118X.2019.1657164

Trepte, S., Scharkow, M., Dienlin, T., 2020. The privacy calculus contextualized: The influence of affordances. Comput. Human Behav. 104. doi:10.1016/j.chb.2019.08.022

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, Reforming European Data Protection Law. Springer, Dordrecht, 333–365.

Vermeulen, G., Lievens, E. 2017. Data protection and privacy under pressure: transatlantic tensions, EU surveillance, and big data: Maklu.

Waldman, A.E., 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. Curr. Opin. Psychol. 31, 105–109. doi:10.1016/j.copsyc.2019.08.025

Walrave, M., Heirman, W., 2013. Adolescents, online marketing and privacy: Predicting adolescents' willingness to disclose personal information for marketing purposes. Child. Soc. 27(6), 434–447. doi:10.1111/j.1099-0860.2011.00423.x

Weinberger, M., Zhitomirsky-Geffet, M., Bouhnik, D., 2017. Factors affecting users' online privacy literacy among students in Israel. Online Inform. Rev. 41(5), 655–671. doi:10.1108/OIR-05-2016-0127

Wright, P., Friestad, M., Boush, D.M., 2005. The development of marketplace persuasion knowledge in children, adolescents, and young adults. J. Public Policy Mark. 24(2), 222–233. doi:10.1509/jppm.2005.24.2.222

Xu, H., Luo, X.R., Carroll, J.M., Rosson, M.B., 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decis. Support Syst. 51(1), 42–52. doi:10.1016/j.dss.2010.11.017

Youn, S., 2005. Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. J. Broadcast. Electron. Media 49, 86–110. doi:10.1207/s15506878jobem4901_6

Youn, S., 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. J. Consum. Aff. 43(3), 389–418. doi:10.1111/j.1745-6606.2009.01146.x

Youn, S., Shin, W., 2020. Adolescents' responses to social media newsfeed advertising: The interplay of persuasion knowledge, benefit-risk assessment, and ad scepticism in explaining information disclosure. Int. J. Advert. 39(2), 213–231. doi:10.1080/02650487.2019.1585650

Zarouali, B., De Pauw, P., Ponnet, K., Walrave, M., Poels, K., Cauberghe, V., Hudders, L., 2019. Considering children's advertising literacy from a methodological point of view: Past practices and future recommendations. J. Curr. Issues Res. Advert. 40(2), 196–213. doi:10.1080/10641734.2018.1503109

Zhang-Kennedy, L., Baig, K., Chiasson, S., 2017. Engaging children about online privacy through storytelling in an interactive comic. Proceedings of the 31st British Computer Society Human Computer Interaction Conference. doi:10.14236/ewic/HCI2017.45

Zhang-Kennedy, L., Mekhail, C., Abdelaziz, Y., Chiasson, S., 2016. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. Proceedings of the the 15th International Conference on Interaction Design and Children. doi:10.1145/2930674.2930716

Zhao, F., Egelman, S., Weeks, H.M., Kaciroti, N., Miller, A.L., Radesky, J.S., 2020. Data collection practices of mobile applications played by preschool-aged children. JAMA Pediatr. 174(12). doi:10.1001/jamapediatrics.2020.3345

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. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1–13).

Figures

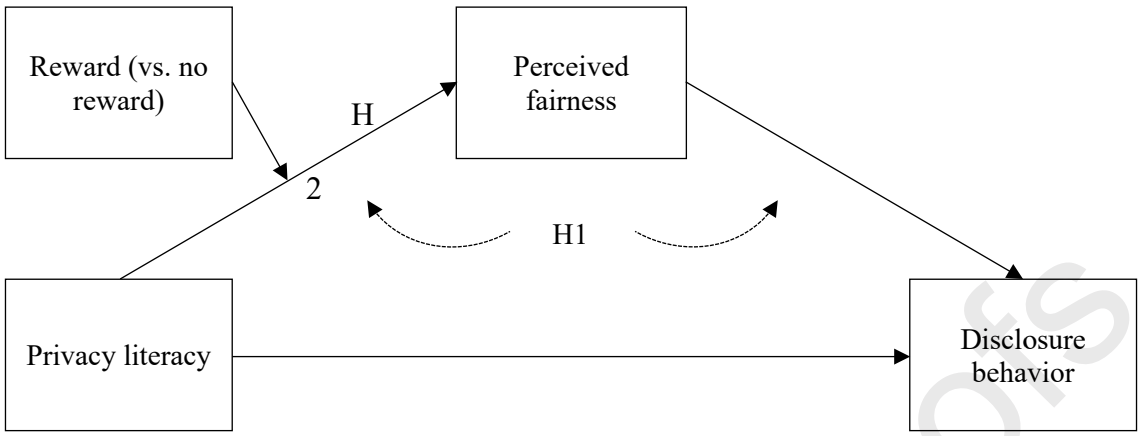


Figure 1: Conceptual model.

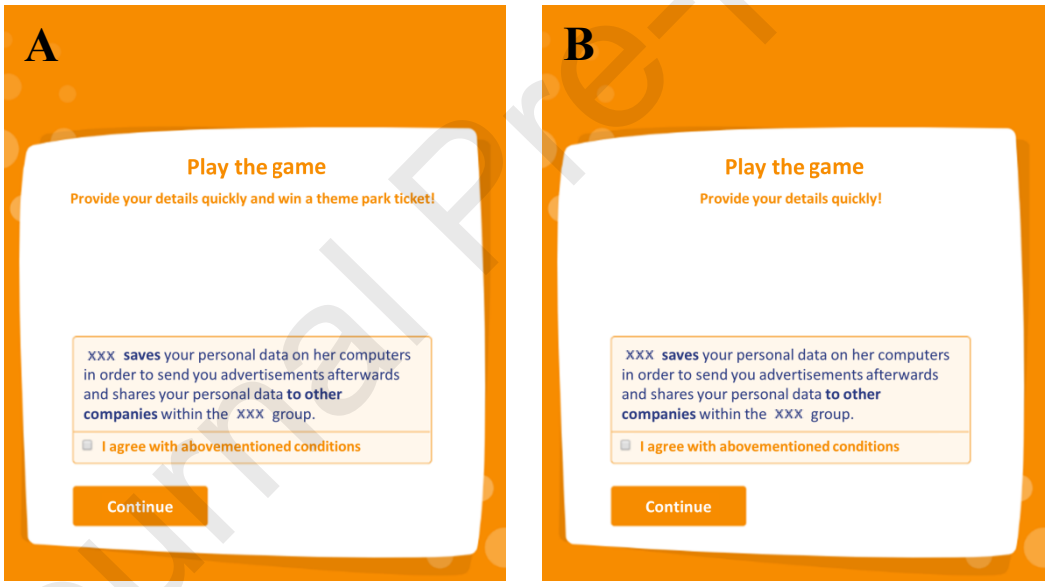


Figure 2: The first page, in which the (a) reward vs. (b) no reward condition is manipulated.

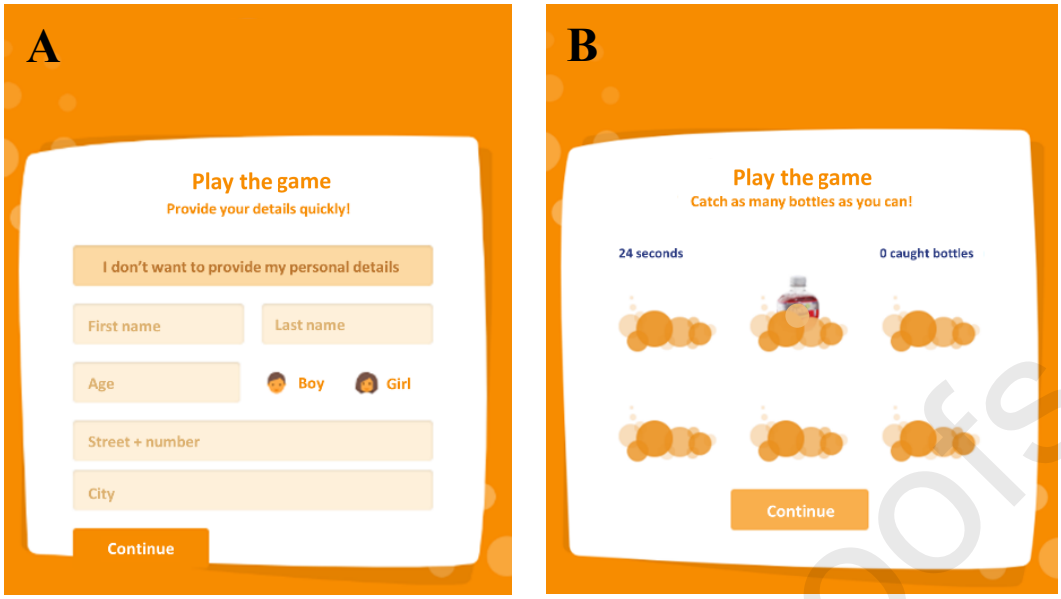


Figure 3: (a) Second and (b) third pages of the website. These pages were the same for all conditions.

Figure 4: Screenshots taken from (a) the privacy literacy training video and (b) the control video.

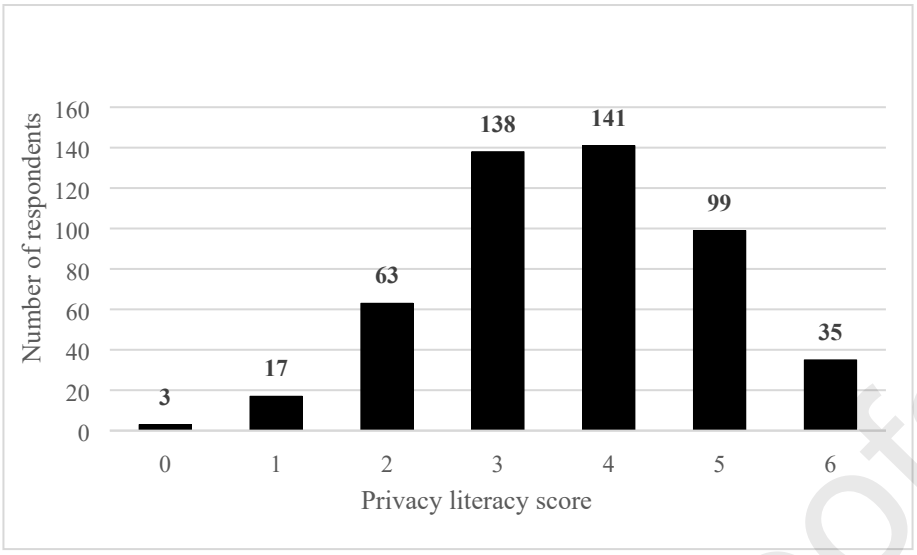


Figure 5: Distribution of the score for privacy literacy (range: 0–6).

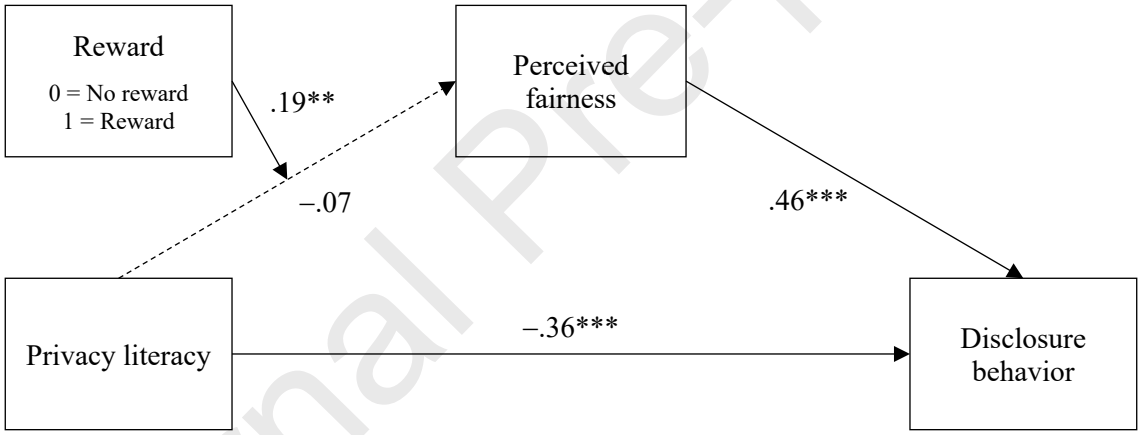


Figure 6: The relationship between privacy literacy and disclosure behavior mediated through perceived fairness and moderated by reward. *p < .05, **p < .01, ***p < .001.

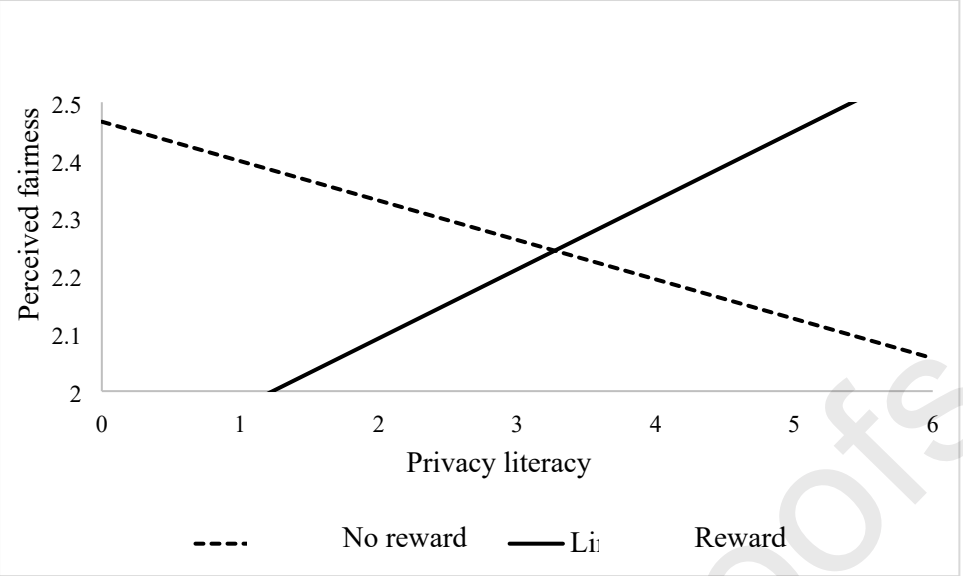


Figure 7: Interaction effects between privacy literacy and reward on perceived fairness. A significant positive effect for privacy literacy on perceived fairness was only observed for the reward condition.

Tables

Table 1: Mean scores on reward liking and value for the different rewards.

Measure	Reward type	Mean	SD
Reward liking (5 points)	Movie ticket	4.57	1.13
	Tennis racket	3.34	1.55
	Comic strip	3.45	1.42
	Theme park ticket	4.58	1.18
Reward value (5 points)	Movie ticket	4.19	0.82
	Tennis racket	2.95	1.29
	Comic strip	2.97	1.21
	Theme park ticket	4.38	1.07

Table 2: Correlations

	Privacy literacy	Perceived fairness	Perceived advantage	Disclosure behavior
Privacy literacy	3.68 (1.26)	.043	–.080	–.175***
Perceived fairness		2.26 (1.08)	.388***	.185***
Perceived advantage			2.42 (1.04)	.355***
Disclosure behavior				1.90 (2.62)

*p < .05; **p < .01; ***p < .001. Diagonal line: Means (SD).

Table 3: Overview of Model 4 (Hayes).

Effect Type	Effect (SE)	LLCI	ULCI
Direct effect of privacy literacy on disclosure behavior	−.36 (.09)	−.5437	−.1854
Direct effect of perceived fairness on disclosure behavior	.46 (.11)	.2498	.6644
Indirect effect of privacy literacy on disclosure behavior through perceived fairness	.02 (.02)	−.0179	.0611

SE:; LLCI:; ULCI:.

Table 4: Overview of Model 7 (Hayes).

Effect Type		Effect (SE)	LLCI	ULCI
Interaction effect between privacy literacy and reward provision on perceived fairness		.19 (.08)	.0326	.3376
Conditional indirect effect for privacy literacy on disclosure behavior through perceived fairness	Reward	.06 (.03)	.0078	.1185
	No reward	−.03 (.03)	−.0970	.0275

SE:; LLCI:; ULCI:.