12-2019

Children and Online Privacy Protection: Empowerment from Cognitive Defense Strategies

J. Craig Andrews
Marquette University, craig.andrews@marquette.edu

Kristen L. Walker
California State University

Jeremy Kees
Villanova University

Special Issue Research Article

AMERICAN MARKETING ASSOCIATION

Journal of Public Policy & Marketing
1-15

DOI: 10.1177/0743915619883638
journals.sagepub.com/home/ppo
SAGE

Children and Online Privacy Protection: Empowerment from Cognitive Defense Strategies

J. Craig Andrews, Kristen L. Walker, and Jeremy Kees

Abstract

At present, very little is known about what might encourage children and teens to limit access to their private information online and to restrict what they share on social media and video sites. Federal and state agencies face challenges encouraging companies to help children, teens, and parents protect their information online. The authors extend previous cognitive defense research by examining (1) effects beyond advertising as applied to information privacy online; (2) not only children's/teens' beliefs and knowledge, but also their online privacy decisions; (3) multiple age categories; (4) multiple cognitive defense strategies (educational video, quiz with feedback, or absence of a strategy); and (5) children's/teens' motivation to restrict what they share online. Key results indicate significant effects of the quiz and educational video over the absence of a strategy in enhancing favorable online safety beliefs and in restricting online sharing. Findings also demonstrate the role of perceived parental influence and for agencies to offer privacy education campaigns to help empower children to protect their privacy. Implications for policy and privacy research are discussed.

Keywords

children, privacy, cognitive defenses, active protection, (self) regulation

Children and Teens Online: A Privacy Problem

Currently, 95% of teens have access to a smartphone, and 45% report that they are online "almost constantly" (Pew Research Center 2018). Children's and teens' online use has reached record highs, with youth aged 5–15 years spending over 15 hours each week online—overtaking time spent watching traditional TV (Ofcom 2017). Even preschoolers, aged 3–4 years, are spending almost eight hours per week online. Parents also are spending a great deal of time online, and some admit that they also struggle with the allure of screens and are increasingly distracted by their devices (Pew Research Center 2018).

Given this almost incessant online activity for many, several questions and challenges emerge. Are children, teens, and parents protecting their online data themselves, and if so, how are they protecting their personal information during online exchanges? If they are not protecting their online information, who is or who should? Are there ways to empower children and teens regarding their online safety knowledge and behaviors? Is it better to have children learn online safety themselves or have parents enforce safety measures? We examine these issues experimentally by testing whether certain cognitive defense strategies (e.g., an educational video, a quiz with feedback) versus an absence of a strategy will help children and teens improve (1) their beliefs about online safety and (2) their decisions to restrict the sharing of videos online. Our focus is on one of the most popular social media sites for children and teens today: YouTube. Our contribution extends prior research on the use of cognitive defense strategies (cf. Brucks, Armstrong, and Goldberg 1988; John 1999; Rozendaal, Buijzen, and Valkenburg 2009) by focusing on information privacy (vs. advertising) and by our testing of specific online safety beliefs and decisions, multiple age categories, and multiple defense strategies, as well as accounting for children's and teens' motivation to restrict access and sharing. We also examine whether children's and teens' perceived parental

J. Craig Andrews is Professor and Charles H. Kellstadt Chair in Marketing, Marquette University, USA (email: craig.andrews@marquette.edu). Kristen L. Walker is Professor of Marketing, California State University, Northridge, USA (email: kristen.walker@csun.edu). Jeremy Kees is Richard J. and Barbara Naclerio Endowed Chair in Business, Villanova University (email: jeremy.kees@villanova.edu).

restrictions on their online viewing and sharing vary by age. Understanding this process of empowerment can help federal and state agencies and marketers improve regulatory efforts to better protect the online privacy of children and teens.

Children's Online Behavior, YouTube, and Company Responses

The privacy of children and teens, and the information collected from them online, represents one of parents' top concerns today (Anderson 2019). There is good reason for this concern, as across all social network profiles, only 61% of youth aged 10–18 years have enabled the privacy settings to protect their content, and 52% do not turn off their location or GPS services across apps, leaving their locations visible to others (McAfee 2014). In addition, 14% posted their home addresses online—a 27% increase from the previous year's results. Even with the Federal Trade Commission's (FTC) Children's Online Privacy Protection Rule (FTC 1998 and updates), a study of online children's apps showed that more than 50% of the apps failed to protect the children's data (Egelman 2017). Recently, operators of the children's app Musical.ly (also known as Tik Tok) agreed to pay $5.7 million to settle FTC charges that they violated the Children's Online Privacy Protection Rule by collecting personally identifiable information from children through the app (U.S. v. Musical.ly and Musical.ly, Inc. 2019). Also, gaming chat apps (e.g., Discord) have been singled out for their lack of age verification and violent messaging and content from users aimed at children and teens (Jargon 2019). Finally, Google's YouTube agreed to a $170 million settlement with the FTC and New York Attorney General based on a complaint that YouTube collected personal information from children for use in behavioral advertising delivered to viewers of children's channels on YouTube (FTC 2019; U.S. and New York Attorney General 2019).

YouTube represents the most popular site for children and teens to view video content, with 73% of those aged 5–15 using the site (Ofcom 2017) and an even higher percentage for teens in general at 85% (Pew Research Center 2018). Google's YouTube is of particular interest for research about children and privacy because it offers two different sites with different target segments. One is considered a "general site" and is directed toward consumers over the age of 13, whereas the other site, YouTube Kids, was introduced in 2015 for children preschool age and older. In 2018, a coalition of consumer advocacy groups complained that YouTube has known that children aged 12 and younger access the general site (instead of YouTube Kids), accusing YouTube of violating the Children's Online Privacy Protection Act (COPPA) (COPPA 1998). As previously noted, this resulted in Google's YouTube settling with the FTC and New York Attorney General for the largest COPPA penalty since Congress enacted the law in 1998 (FTC 2019).

Although parents claim they check what their teens and children do online and post on social media (Anderson 2019), recent reviews of the most popular video websites (e.g., YouTube) indicate that child protection mechanisms are breaking down (Wendling 2017). For example, YouTube's volunteer "Trusted Flaggers[1]" report that of 526 complaints made to YouTube's public reporting abuse page, only 15 responses were received back from the service (Wendling 2017). The reports were made primarily against accounts that left objectionable comments (often sexually explicit) on videos made by young teenagers and children. As a result, YouTube promised to increase its transparency with users about how it flags videos and handles reports about flagged videos. The first "Community Guidelines Enforcement Report," covering the last quarter of 2017, indicates that the general site (i.e., not YouTube Kids) removed approximately 8.2 million videos during that period (Shu 2018). Some consumer advocacy groups have noted that although "YouTube Kids may be more 'kid-friendly' than YouTube itself," the site is "still technically a portal to the main YouTube service," which contains a considerable amount of questionable content (Common Sense Media 2018). In essence, privacy protection (i.e., control and access to personal information) is still primarily the responsibility of parents and the children themselves. Empowering children to set limits for their online interactions is a key factor, especially for those on YouTube. Our study contributes to these areas by examining what types of cognitive defense strategies can be effective at improving online safety beliefs for children and teens and, in turn, helping them to restrict the sharing of private information.

Regulatory Efforts in Protecting Children's Online Privacy

Since 1997, the Federal Trade Commission (1997) and industry self-regulatory guidelines for children (Children's Advertising Review Unit (CARU) 1997), have recommended providing (1) full and effective *notice* or disclosure (e.g., regarding the information collected, how it will be used, information access), (2) parental or guardian *consent*, (3) parental or guardian choice (*access*) with respect to the information collected, and (4) future privacy protection (*security*) for children. These four privacy principles are now enforced as part of the FTC's Children's Online Privacy Protection Rule (FTC 1998; emanating from the Children's Online Privacy Protection Act or "COPPA" 1998), which applies to any website collecting data from children under age 13 in the United States. COPPA offers guidelines for websites targeting children to ensure parental consent for children aged 13 and under; however, a loophole exists for websites that target general audiences, which children may still access. California recently addressed this loophole with The California Consumer Privacy Act of 2018 (AB 375), which extends the protection to children/teens under age

[1] "YouTube Trusted Flagger program was developed by YouTube to help provide robust tools for individuals, government agencies, and nongovernmental organizations (NGOs) that are particularly effective at notifying YouTube of content that violates [the] Community Guidelines." (support.google.com).

16 and requires prior parental permission for sites to collect children's data. Either way, this type of regulation and legislation focuses on protecting the data gathered and advertising delivered to users on websites targeting children, rather than constraining the amount of data gathered. This represents an important distinction affecting the ability of parents and children to protect their exchanged information.

Since COPPA (1998, with 2012 amendments included) and AB 375, there have been privacy workshops and conferences (PrivacyCon) almost every year at the FTC centered on these issues (e.g., "Putting (Privacy) Disclosures to the Test," FTC 2016). Although these privacy principles, workshops, and conferences are intuitively appealing, very little research has been conducted to examine how children and teens actually respond to privacy disclosure information and education.[2] This is a significant gap in research, as children and parents are increasingly relying on devices and online connections to give them the power to accomplish tasks and assist with daily responsibilities. Thus, important questions remain regarding how children store, retrieve, and make choices regarding their online information (e.g., parental permission), warning information (e.g., not to post full names, phone numbers, email addresses), and restrictions to content posted. In this study, we examine experimentally whether cognitive defense strategies (e.g., an educational video, a quiz with feedback) will positively influence children's online privacy knowledge and willingness to place conditions on what they might share and whether they restrict access to videos watched. First, we discuss research on what motivates children's and teens' (online) decision making and why they often resort to risk taking. Then, we present efforts to help reduce such (online) risk taking, such as the active setting of privacy controls through cognitive defense strategies.

Children's and Teens' (Online) Decision Making

Research has shown that children and adolescents (aged 13–17 years) are more impulsive, self-conscious, prone to risk taking, and more vulnerable to harm than adults (Pechmann et al. 2005; Steinberg 2020). A primary reason for this is the rapid development and plasticity of the brain in these formative years (Pechmann et al. 2005). The release of dopamine plays an important role in adolescent neural activity in response to novel stimuli and rewards (e.g., social media postings, comments and likes, text pings, Twitter bird whistles). As such, adolescent choices are driven more by rewards during this period than by an evaluation of risks (Steinberg and Scott 2003). For example, research has shown that adolescents (aged 13–17) have significantly higher intentions to take online risks (e.g., disclosing personal information, making unknown friends online) than young adults (aged 18–24) (White et al. 2015). One reason for this is that the prefrontal cortex, important for inhibitory control and objective risk assessment, is not fully developed until late adolescence. Moreover, the skills required to control urges found in adolescence are not developed until later—often leading to risky decisions (Pechmann et al. 2005).

Fitting in socially is an additional pressure that children and adolescents often face online. Peer influence, often manifested through social media, is at its strongest in early adolescence and only slowly declines in high school (Steinberg and Scott 2003). Due to this period of impulsivity, sensation seeking, self-consciousness, and peer influence, adolescents are particularly vulnerable to making poor decisions, leading to an elevated risk of addiction (e.g., social media) and other abuses (Andrews and Netemeyer 2015; Pechmann et al. 2005). Adolescents also are shown to be more susceptible to advertising imagery and consumption symbols for harmful products (cf. Pechmann and Knight 2002; Pollay et al. 1996). Ideally, the development of one's knowledge of advertising tactics and appeals (i.e., persuasion knowledge; Friestad and Wright 1994) can help reduce such susceptibility. However, as noted by Friestad and Wright (1994), such persuasion knowledge, involving more abstract, skeptical, multidimensional, and less absolute thinking, only begins to form in adolescence and develops slowly. Also, in the study of adolescent online risk taking, White et al. (2015) find that verbatim (absolute) representations correlate positively with online risk intentions, whereas gist (meaning) representations correlate negatively with such online risk intentions. So, how is such online knowledge and meaning developed by children and adolescents? The answer may lie in the development and activation of privacy protection (Walker 2016), digital/media literacy (Hobbs 2011; Pechmann et al. 2005), and/or cognitive defense strategies (Brucks, Armstrong, and Goldberg 1988) to empower children and adolescents online.

Active Versus Passive Privacy Protection

Efforts to encourage active (vs. passive) privacy protection by educating parents and children about privacy issues have become more prominent recently. As such, privacy education is encouraged strongly by industry and public policy to achieve what is considered "digital literacy" (Hobbs 2011). Digital literacy involves not only the ability (for youth) to understand the risks involved when providing information online but also to understand immediate dangers involving other people, such as cyberbullying, stranger danger, etc. COPPA is an attempt to address the general issue of the collection and use of information by websites, apps, and platforms. But, as discussed previously, COPPA is limited to children under age 13 (16 and under in California) and only requires sites to obtain parental permission to gather data. Industry efforts tend to focus on complying with COPPA and ensuring websites avoid collecting personal information and engaging in online behavioral advertising when such sites have "actual knowledge" that users are under the age of 13 (Interactive Advertising Bureau 2015, p. 5). The

[2] Research on children also can be challenging because they are considered a specially protected group (i.e., academic research requires approval from an institutional review board).

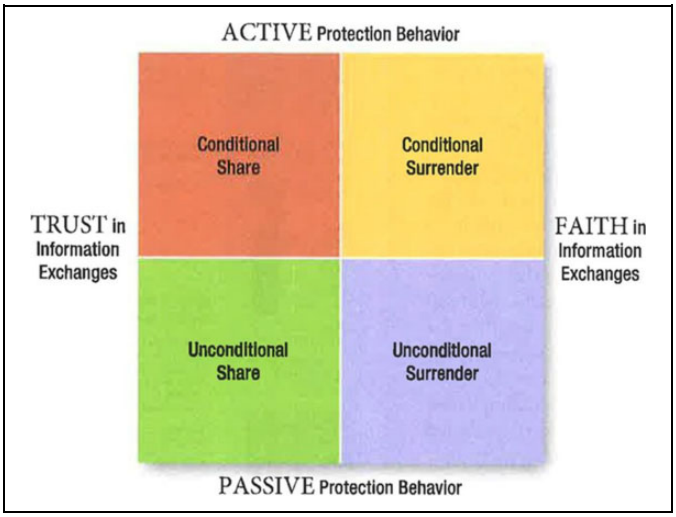

Figure 1. Consumer information privacy: The sharing–surrendering information matrix. Source: Walker (2016).

purpose of improving one's digital literacy is to strengthen the competence and understanding of digital knowledge, skills, and attitudes, including the protection of personal information exchanged. Using strategies to strengthen children's cognitive defenses supports digital literacy efforts to help them protect their privacy online.

To aid in research and discussion on active privacy protection, Walker (2016) portrays the uncertainty about the exchange of information and the levels of privacy protection in a 2 × 2 matrix of sharing–surrendering information (SSIM; see Figure 1). In the SSIM, privacy protection levels are displayed along a continuum of active or passive based on how many conditions individuals use, place, enact, etc. when exchanging information. An individual who is active in their privacy protection may place conditions on their exchanges by using privacy settings, employing different email accounts for app use, viewing online content with private mode(s), etc. When an individual is passive in their protection and does not place conditions on their online exchanges of information, they are unconditionally exchanging information.

As an example of passive protection and unconditional sharing, consider the situation in which a child/teen downloads a new app on a smartphone and quickly checks the privacy terms box assuming there is no harm from the app's collection of information. Unfortunately, improving the ability of individuals to process and actively protect privacy often has been relegated to the assumed reading of privacy policy disclosure notices. But such notices are widely criticized as being anything but "clear and conspicuous," as they often appear in small type size, are lengthy, are not clearly written, and at times are not presented with the target audience in mind (e.g., children, older consumers) (Hoy and Andrews 2004). So, how can agencies improve the digital literacy, readability, and processing of important online privacy information, especially with children and teens in mind? Some studies have pointed to the superiority of dual modality—the simultaneous presentation of a message in audio and video—in affecting awareness, comprehension, knowledge acquisition, and recall of information (cf. Hoy and Andrews 2004). This superiority assumes that dual modality enhances one's depth of message processing in contrast to a single mode of presentation (i.e., either solely in audio/written form or only in video form; Paivio 1969). But, again, dual modality is still only an enhancement in a condition of passive (vs. active) privacy protection.

Overall, the SSIM extends the level of protection beyond passive and acknowledges a difference in how much people trust their online interactions. Yet, in our study, we focus on how to activate cognitive defense strategies in children that will encourage them to place conditions on their exchanges of information in the hope that they will become active in their privacy protection.

Cognitive Defense Strategies to Improve Privacy Knowledge and Decisions

As originally conceived, children who can understand the selling intent of advertising are said to have developed "cognitive defenses" (Brucks, Armstrong, and Goldberg 1988; Rossiter and Robertson 1974). However, as aptly noted by Brucks, Armstrong, and Goldberg (1988) and John (1999), simply understanding the general selling intent of advertising is not sufficient for being able to resist specific persuasive appeals. For example, "general knowledge and beliefs about advertising cannot be expected to dampen a child's enthusiasm for an enticing snack or toy" (John 1999, p. 190). As applied to our study, general knowledge about the privacy of information may not lessen a child's or teen's desire to download the latest app and/or quickly share personal information online. The cognitive defense needs to be specifically applied to sharing decisions that children or teens make. In addition, a child's or teen's knowledge about advertising or sharing personal information online can only serve as a cognitive defense when it is accessed or activated at the time a child/teen is viewing an ad or sharing information online (cf. Brucks, Armstrong, and Goldberg 1988; John 1999).

As an example, to activate knowledge from educational films about advertising persuasion, Brucks, Armstrong, and Goldberg (1988) used a cueing strategy for children aged 9–10 to bolster their cognitive defenses. This cueing strategy consisted of a five-item quiz asking children whether television commercials make products look larger, work better, seem more fun and exciting, make the children cooler/look better, and make it hard to remember important things about products. They found that over 70% of children's counterarguments to the commercials shown were in the high knowledge-cue present condition as opposed to other conditions in which their cognitive defenses were not cued. Also, and in general, increasing one's ability to process and act on knowledge through defense strategies is more likely to lead to beliefs and attitudes that become internalized, are relatively enduring, are more resistant to counter persuasion, and are more likely to lead to behavior change (Kelman 1961; Petty and Cacioppo 1986).

In our current study, we offer the following incremental contributions to prior cognitive defense research by examining (1) effects beyond advertising as extended to information privacy online; (2) not only children's and teens' beliefs, knowledge, and/or attitudes but also their online privacy decisions; (3) multiple age categories; (4) multiple cognitive defense strategies; and (5) and accounting for children's and teens' motivation to restrict what they share online. In this study, young people's ability to actively restrict access when sharing their private information online is activated by either a short educational video ("Be A Smart Cookie") or quiz with elaborated feedback based directly on the video. Elaborated feedback involves not only providing whether a child/teen answered the quiz question correctly but also explaining *why* (Van der Kleij, Feskens, and Eggen 2015). Researchers have found such feedback to be more effective on learning outcomes than simple statements of whether the answer was correct (Van der Kleij, Feskens, and Eggen 2015). Thus, we believe that the quiz with feedback will result in greater active learning (e.g., belief change) by children and teens about online privacy than the video containing the exact same content or nothing at all.

Motivation and Ability (Age) to Restrict Online Information

The Elaboration Likelihood Model, through its motivation and ability to process dimensions, provides a valuable framework to examine additional factors that might help a person restrict what they share online and the effect of these factors on persuasion and related behaviors (Petty and Cacioppo 1986; see also Andrews 1987; Andrews and Shimp 1990; 2018; Batra and Ray 1986; MacInnis, Moorman, and Jaworski 1991). Our study seeks to tap into two of these important precursors to persuasion: motivation and ability to restrict one's online information.

Motivation to Restrict Online Information

For children and teens, one's prior *motivation* to process and act on information can be an important antecedent to persuasion (Petty and Cacioppo 1986). That is, the personal relevance to children and teens as to whether they should take action in protecting and restricting their personal information is at issue. With greater motivation, they are likely to allocate greater effort in thinking about the consequences of sharing private information and actively place restrictions on such sharing. Those who are more motivated to process and act on their personal information are more likely to develop beliefs and attitudes that become internalized, are relatively enduring, are more resistant to counter persuasion, and that are more likely to lead to behavior change (Kelman 1961; Petty and Cacioppo 1986).

The Role of Age in Ability to Process, Learning Differences, and Reactance

An individual's *ability* to process and act in restricting and protecting their private information online has been discussed in terms of closing "knowledge gaps" and improving literacy on privacy issues (Trepte et al. 2015). In general, the ability to process and act on information is related to one's knowledge, skills, digital literacy, etc. As previously noted, several cognitive defense strategies will be tested to develop and enhance children's and teens' privacy knowledge gaps and digital literacy. However, individual differences, such as education, intelligence, and cognitive development as young people age have been shown to enhance one's ability to process information (Petty and Cacioppo 1986).

For instance, research on children's information processing is useful for digital literacy efforts (Roedder 1981; Gregan-Paxton and John 1997) and proposes three stages of cognitive development for children to separate central and incidental material: limited (under age 8), cued (age 8–12) and strategic (over age 12). (Other age categories were proposed by Roedder for different activities.) Based on this research, Brucks et al. expected that children must reach the strategic processing stage (age 13) before they can generate spontaneous cognitive responses. Children aged 8–12 would need a defense strategy cue or prompt to focus their attention and counterargue. However, children under age 8 (limited category) were predicted to be more challenged than those aged 8-12 in focusing attention on the arguments and counterarguing. Brucks, Armstrong, and Goldberg (1988) extended this research by showing that advertising knowledge did not result in increased counterarguments against advertisements for the cued age group (age 9–10) unless a direct cue was present to activate that knowledge. However, based on research in child development and digital activity (discussed subsequently), we believe that reactance and rebellion experienced at this age to follow online privacy rules will take precedence in attenuating efforts to restrict their sharing of private information in comparison to older age groups.

Early adolescence (e.g., age 8–13) marks a time of serious rebellion against parents, safety rules, and restraints, in which young people reject their "old child identity" (Pickhardt 2009). Such rebellion often goes against their own self-interest in supporting their self-esteem and can lead to self-destructive and high-risk behaviors. This is only exacerbated with increased social media use at this age and can result in negative consequences in this venue. Thus, as children age from more limited knowledge and ability (e.g., from age 6–7 to 8–12), they are likely to exhibit more reactance to rules (Brehm and Brehm 1981) and be less motivated to restrict or limit their private information online. Such reactance is likely to be attenuated with older children/teens due to their greater autonomy, independence, and online experience. Older children/teens (age 13–15) also should be more "tech savvy" in their online privacy protection due to their greater experience with apps, devices, and online information, especially as they reach high school. In a report for the Digital Trust Foundation, research on middle school youth found a "7th grade technology leap" with an "overall increase in device use and online activity" between ages 12 and 13. At this age, friends tend to play a more important role in influencing other children/teens, and this age group

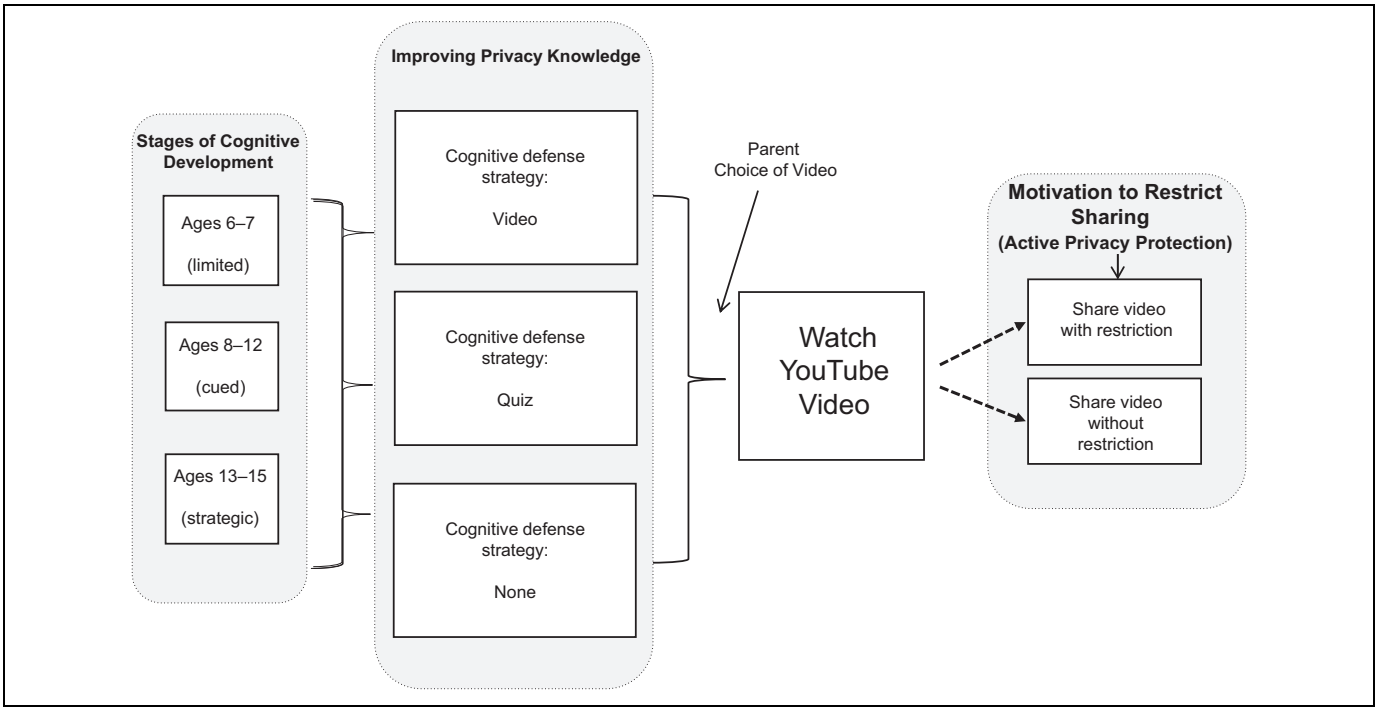

Figure 2. Conceptual study framework: Children's online privacy study process and key variables.

prefers to ask their friends for help about issues online rather than ask their parents or teachers (Walker, Kiesler, and Malone 2016, pp. 22–23). Yet, at times, such independence and/or reliance on other young people may result in misinformation and overconfidence as children/teens age.

Research Focus, Incremental Contributions, and Conceptual Study Framework

Thus, our study extends previous cognitive defense research by: (1) examining a new application area (children's information privacy), (2) including additional age categories (e.g., limited, strategic), and (3) testing multiple cognitive defense strategies to aid online safety knowledge and the ability to place restrictions (conditions) on personal information online. We also believe that (4) a child's or teen's motivation to actively protect their privacy online is an important factor in the process. The process of these key variables is presented in our conceptual study framework found in Figure 2.

Study Predictions

Considering the preceding research, we predict the following:

> **H_1:** The quiz cognitive defense treatment should lead children and teens to (a) have more favorable beliefs about online safety, (b) place greater importance on restricting sharing of the YouTube (YT) video watched, and (c) have greater willingness to restrict sharing access to the YT video watched than the other cognitive defense cue treatments (i.e., video, absence of a cue).

> **H_2:** Children and teens with a higher motivation to restrict their access and sharing (in general) will have (a) more favorable beliefs about online safety, (b) greater understanding of the importance of restricting the YT video watched, and (c) greater willingness to restrict sharing access to the YT video watched than those with a lower motivation to restrict access and sharing (in general).

> **H_3:** The strategic (age 13–15) group should (a) have more favorable beliefs about online safety, (b) place greater importance on restricting sharing of the YT video watched, and (c) have greater willingness to restrict sharing access to the YT video watched than the limited (age 5–6) or cued (age 8–12) groups.

Method

Pretests of Cognitive Defense Strategies and Measures

Prior to the main study, we conducted pretesting to test video and quiz content and measures intended to aid the restriction of information and videos shared online by children and teens. We used a professional marketing research firm with expertise in collecting panel data from children and teens to collect the data online in the pretest and main study. An email solicitation to parent panel members included the survey link, estimated survey time, and the specific minimal reward compensation (gift card points or sweepstakes entry). Panel account information was kept separate from general ID numbers for all data provided. Following screening for age categories (age 6–7; age 8–12; age 13–15), reading ability, parental consent, and

child/teen assent, we used a pretest of 146 children and teens split evenly across age categories and gender to test the video and quiz content. Children/teens were randomly assigned to either (1) a 1-minute, 17-second educational video edited from "Be a Smart Cookie" from YouthPrivacyProtection.org[3] or (2) a seven-item true/false educational quiz ("Tips for Online Safety"; see Appendix A) based directly on information in the video. For the quiz, children/teen respondents were then given feedback as to whether their answer was correct and why this was the case. Pretest results for the quiz ranged from 70.1% to 97.9% correct for the seven items. The video and quiz manipulations worked as intended, with checks measuring whether the video/quiz said, "Every time you go online, a part of yourself is left behind" (video = 95% correct; quiz = 95% correct) and "Third-party shadows follow wherever you click" (video = 85% correct; quiz = 97% correct). Believability of the quiz and video was measured on three seven-point scales (1 = "not believable" through 7 = "believable," 1 = "not credible" through 7 = "credible," and 1= "not trustworthy" through 7 = "trustworthy"; $\alpha_{video} = .90$; $\alpha_{quiz} = .86$). Average believability of the video (x = 5.97 (3.07)) and the quiz (x = 5.97 (3.63)) were above the scale midpoint (4.0). Also, believability did not vary across age categories for the video ($F(2,68) = .026$; $p = .975$) and quiz ($F(2,68) = .045$; $p = .956$). Finally, as a check on the processing fluency of both the video and quiz (Schwarz 2004), respondents were asked four seven-point questions (1 = "tough to understand" through 7 = "easy to understand," 1 = "tough to process" through 7 = "easy to process," 1 = "unorganized" through 7 = "organized," and 1= "unclear" through 7 = "clear"; $\alpha_{video} = .93$; $\alpha_{quiz} = .81$). Average processing fluency of the video (x = 6.00 (4.37) and quiz (x = 5.92 (4.74)) were both above the scale midpoint (4.0). In addition, processing fluency did not vary across age categories for the video ($F(2,68) = 1.64$; $p = .202$) and quiz ($F(2,63) = .661$; $p = .520$).

Main Study: Sample and General Procedure

The main study consisted of 513 children and teens split evenly across the same three key age groups (6–7, 8–12, and 13–15) and gender (50.4% female; 49.6% male). The ethnic breakdown was 68.9% Caucasian (not Hispanic), 11.9% Hispanic, 10.9% African American (not Hispanic), 4.7% Asian American, and 3.6% other ethnicities. The median category reported for time spent online was 1–2 hours per day. The same vendor and procedures used in collecting pretest data were used in the main study. Those participating in the pretest were not part of the main study. The children/teens (with parental consent and child/teen assent) were recruited and screened for ability to read, current availability, presence of a parent or guardian, and parental possession of a YouTube account. Following parental agreement to the interview, the children/teens were randomly assigned to a cognitive defense strategy from the pretest—either the video clip on online privacy safety (see link provided in footnote 3), the educational quiz on online privacy safety (see Appendix A), or nothing at all (i.e., the control). The information on online safety presented in both the video and educational quiz cues was identical. The main study results for the seven-item quiz ranged from 75.2% to 98.2% correct. As in the pretest, we used processing checks to make sure participants indeed viewed the cognitive defense strategy if they were assigned to one (i.e., the online safety video or quiz) and watched the YouTube video. For the main study, the video and quiz manipulations worked as intended, with checks measuring whether the video/quiz said, "Every time you go online, a part of yourself is left behind" (video = 90% correct; quiz = 96% correct) and "Third-party shadows follow wherever you click" (video = 75% correct; quiz = 96% correct).

Children/teens were later (with parent permission) allowed to view an age-appropriate video on YouTube that was first selected by a parent. Before viewing the YouTube video, they were asked if their parents restricted what they watch on YouTube. Parents were then instructed to open their YouTube account, find an age-appropriate video for their child/teen to watch, and step aside while the child/teen watched it and then answered questions. After viewing the video for a maximum of one to two minutes, we asked the children/teens filler questions regarding what the video was and whether they liked it. A total of 90.3% of the children/teens liked the video that was selected for them to watch. We then asked the children/teens a key question; i.e., whether or not they wanted to share the YouTube video. If yes, they were asked about options for restricting who they share the video with (e.g., with everyone, only family and friends, only parents, no one). We then assessed their beliefs regarding the importance of restricting who they might share the video with, as well as five specific beliefs about online safety that were tailored to the information presented in the video and quiz. Finally, we measured parents' views about restricting their own online information and that of their teen/child, as well as the teen's/child's online and app usage and other demographic information.

Main Study: Key Independent Variables

The main study consisted of nine cells in a 3 (*cognitive defense strategy*: video, quiz, or absent [control]) × 3 (*age difference category*: limited: age 6–7, cued: age 8–12, or strategic: age 13–15) design. The total sample of 513–with 57 per cell–offered an 88% chance of detecting a medium-sized effect (e.g., omega-squared of .25) with a 5% estimate of error (Cohen 1969, p. 309). We used a median split on *motivation to restrict online information* (in general) to separate child/teen respondents into high and low motivation-to-restrict groups. This motivation to restrict online information (in general) was a mean-centered, summated scale measured with three seven-point agreement items: "It is important that I restrict what I am doing and sharing online," "I am interested in restricting what I am doing and sharing online," and "I am motivated to restrict what I am doing and sharing online" ($\alpha = .90$).

[3] Video clip available at https://www.youthprivacyprotection.org/cookie-video-clip.

Table 1. Multivariate and Univariate Results: Online Safety Beliefs and Importance of Restricting YouTube Video Watched.

	MANOVA Results[a]			Univariate Results			
Independent Variables	Wilks' λ	F-Value	Partial Eta-Squared	Online Safety Beliefs	Partial Eta-Squared	Importance of Restricting YT Video	Partial Eta-Squared
Main Effects							
Cognitive defense strategy (CDS)	.93	8.40***	.04	15.21***	.06	2.62*	.01
Age category (A)	.96	.88	.01	1.34	.01	.51	.00
Motivation (M)	.82	51.04***	.18	91.32***	.16	15.06***	.03
Interaction effects							
CDS × A	.98	.94	.01	.75	.01	1.06	.01
M × A	.99	1.18	.01	1.50	.01	1.94	.01
CDS × M	.99	.07	.00	.02	.00	.11	.00

[a]***$p < .01$; **$p < .05$; *$p < .10$, N = 513.

Note: Three-way interactions are nonsignificant for both dependent measures.

Main Study: Dependent Measures and Analysis

Before the children/teens watched the YouTube video selected by their parents, we asked them if their parents restricted what they watched on YouTube. Later, after viewing the YouTube video, two key categorical dependent variables assessed the teen's/child's decisions regarding the YouTube video they watched. These assessed whether they would (1) share the video ("Would you like to share the video with others?") and, if yes, (2) with whom ("Who would you share the video with?"; everyone, only family and friends, only parents, no one). The importance of the teen/child restricting with whom they might share the video was measured on a seven-point scale (1 = "not important at all" through 7 = "very important"). Also, five specific online privacy beliefs were measured on seven-point agreement scales: (1) "When you go online, part of you never goes away (e.g., posts, likes, searches)," (2) "Third party 'shadows' see what you are doing online," (3) "Online sites share your information with third-party 'shadows,'" (4) "Third-party 'shadows' give your information to companies that target you (e.g., send ads to you)," and (5) "You should keep your personal information out of the hands of people who don't know you." We created a mean-centered, summated scale of the online safety beliefs ($\alpha = .85$).

A multivariate analysis of variance (MANOVA) was used to examine the impact of the independent variables on the online safety belief and importance of restricting the YT video measures. Given overall significance, we performed follow-up Student-Newman-Keuls (SNK) contrasts in accordance with predictions in the hypotheses. Means and standard deviations are provided for each treatment group. We used chi-square analysis and logistic (logit) regression for the categorical decision measures.

Results

Online Safety Beliefs

For beliefs about online safety and the importance of restricting sharing of the YouTube video, we conducted a MANOVA to examine the effects of the cognitive defense strategy treatment, age categories, and motivation to restrict the exchange of online information (in general). Table 1 displays the overall multivariate and univariate findings for the effects of these independent variables on the belief and importance measures. The means and standard deviations for the independent variables appear in Table 2.

H_{1a} predicted that the quiz cognitive defense treatment would lead to more favorable beliefs about online safety than the other cognitive defense cue treatments (i.e., video and absence of a cue). In support of H_{1a}, and as shown in Table 2, an SNK contrast indicated that the quiz defense treatment (M = 6.21) led to significantly greater online safety beliefs than the video defense treatment (M = 5.84; $p < .05$) and the control (M = 5.46; $p < .05$). In support of H_{2a}, and as shown in Table 2, those children/teens with a higher motivation to restrict sharing (M = 6.29) had significantly greater online safety beliefs than those with lower motivation levels (M = 5.31; $p < .05$). As indicated in Table 2, the predictions in H_{3a} were supported, as the teens aged 13–15 (M = 6.01) had significantly greater online safety beliefs than the children aged 8–12 (M = 5.75; $p < .05$) and children aged 6–7 (M = 5.61; $p < .05$). There were no differences between the children aged 5–6 (M = 5.50) and the children aged 8–12 (M = 5.54; $p > .05$). The cognitive defense strategy findings were robust in holding within each age group and motivation to restrict group.

Importance of Restricting the Sharing of the Specific YouTube Video Watched

We asked the children and teens about the importance of restricting the sharing of the specific YT video they had watched. As indicated in Table 2, H_{1b} was supported in part, with the quiz cognitive defense treatment (M = 5.04) leading to a significantly greater importance of restricting the sharing of the YT video watched than the control (M = 4.51, $p < .05$). However, the quiz did not lead to a significantly greater importance of restricting the YT video watched than the educational video (M = 4.75, $p > .05$). In support of H_{2b}, those with a

Table 2. Means (and SDs): Effects of Cognitive Defense Strategy (CDS), Age (A), and Motivation (M) Conditions on Online Safety Beliefs and Importance of Restricting the YT Video.

	Online Safety Beliefs	Importance of Restricting YT Video
Cognitive Defense Strategy		
Control (a)	5.46 (1.26)[b,c]	4.51 (2.16)[c]
Video (b)	5.84 (1.03)[a,c]	4.75 (1.97)
Quiz (c)	6.21 (0.94)[a,b]	5.04 (2.01)[a]
Age Category		
Age 6–7 (a)	5.61 (1.23)[c]	4.64 (2.16)
Age 8–12 (b)	5.75 (1.21)[c]	4.68 (2.02)
Age 13–15 (c)	6.01 (0.97)[a,b]	4.90 (2.07)
Motivation		
Low (a)	5.31 (1.08)[b]	4.30 (1.81)[b]
High (b)	6.29 (1.02)[a]	5.20 (2.24)[a]

Note: Comparisons are made going down a column. Superscripts adjacent to the means for a given column in the table indicate significant differences (p .05 or better) according to SNK contrasts based on predictions. For example, for the online safety beliefs column and comparing cognitive defense strategy treatments, the superscript for the "c" cell (quiz) indicates that the online safety belief mean is significantly greater than the means for both the control cell labeled "a" and the video cell labeled "b."

higher motivation to restrict access and sharing in general (M = 5.20) gave a significantly higher importance to restricting the sharing of the specific YT video they watched than those with a lower motivation to restrict access and sharing in general (M = 4.30, $p < .05$). Finally, although in the predicted direction, yet not supporting H_{3b}, teens age 13–15 (M = 4.90) did not place a significantly greater importance on restricting sharing of the YT video they watched than children age 8–12 (M = 4.68) or age 6–7 (M = 4.64, $p > .05$).

Sharing the YouTube Video watched

Children/teens were asked if (1) they would share the YouTube video they watched and, if yes, (2) with whom. This first decision question was used to test predicted relationships in H_{1c} through H_{3c}. Regarding *sharing the YT video*, a chi-square analysis revealed a significant relationship between agreeing to share the YT video watched and the cognitive defense condition (χ^2 (2) = 6.921, $p < .05$; control = 84%, quiz = 75%, video = 72%). We then conducted logistic regression to examine the specific effects of each cognitive defense condition (vs. the control) on children's/teens' willingness to share the YT video. In partial support of H_{1c}, the children/teens in the control condition were significantly more likely to be willing to share the YT video they watched than those in the quiz condition (84% vs. 75%, odds ratio [OR] = 1.755, $p < .05$, [95% CI, 1.02–3.02] and those in the video condition (84% vs. 72%, OR = 2.016, $p < .05$, [95% CI, 1.15–3.55]). However, there were no differences between those in the quiz (75%) versus video (72%) conditions (OR = 1.15, $p > .05$, [95% CI, .66–2.01]).

Those who were higher in motivation to restrict sharing (in general) were found not to differ in willingness to share the YT video (76.7%) from those who were lower in motivation to restrict access and sharing (in general) (78.8%; (χ^2 (1) = .286, $p = .59$). A logistic regression did not support the prediction in H_{2c} of a positive relationship between motivation to restrict sharing (in general) with the teen's/child's willingness not to share the YT video (OR = 1.13, $p = .593$, [95% CI, .72–1.77].

For age, a chi-square analysis indicated that the children age 8–12 had greater willingness to share the YT video they watched (81.8%) than the teens aged 13–15 (72.3%) and the children age 6–7 (79.9%), although an overall chi-square test did not reach significance (χ^2 (2) = 4.31, $p = .12$). Individual logistic regressions first revealed support for H_{3c}, as the strategic age group of teens age 13–15 were significantly less likely to share the YT video they watched (72.3%) than the cued age group of children age 8–12 (81.8%; OR = 1.717, $p < .05$, [95% CI, .99–2.98]). However, although in the predicted direction, the teens age 13–15 were not significantly less likely to share the YT video they watched (72.3%) than the limited age group of children age 6–7 (79.9%; OR = .418, $p = .131$, [95% CI, .88–2.62]).

Setting Boundaries for Sharing (Restricting the Audience)

Those willing to share the YT video they watched were then asked *who they were willing to share the YT video* with (e.g., everyone, only friends and family, no one). In an examination of the cognitive defense strategy, a chi-square analysis indicated that those in the quiz condition were more likely to share the YT video watched with *everyone* (44.8%) than those in the control (38.3%) or those exposed to the video (30.0%), although an overall chi-square test did not reach significance (χ^2 (2) = 4.16, $p = .12$). A logistic regression revealed that the children/teens in the quiz condition were significantly more likely to be willing to share the YT video they watched with *everyone* (45.4%) than those in the video condition (30.0%; OR = 1.891, $p < .05$, [95% CI, 1.02–3.49]). However, there were no differences in the likelihood of sharing with *everyone* between the control (38.3%) and quiz conditions (44.8%; OR = .77, $p = .30$, [95% CI, .46–1.27]) and between the control (38.3%) and video conditions (30.0%; OR = 1.449, $p = .20$, [95% CI, .81–2.58]).

Although both percentages were lower, those who were higher in motivation to restrict their sharing (in general) were found (somewhat surprisingly) to have a greater willingness to share the YT video with *everyone* (46.0%) versus those who were lower in motivation to restrict sharing (in general) (31.5%; χ^2 (1) = 7.52, $p < .05$). This counterintuitive result may be due to overconfidence on the part of youth in handling online safety themselves and through their network of friends. A logistic regression indicated that those with higher motivation to restrict sharing (in general) were more willing to share the YT video with *everyone* (46%) versus those with low motivation (31.5%) (OR = .54, $p < .05$, [95% CI, .35–.77]).

Finally, the percentage of those who were willing to share the YT video they watched with *everyone* increased with age,

with 6- to 7-year-olds at 31.9%, 8- to 12-year-olds at 36.7%, and 13- to 15-year-olds at 47.2% (χ^2 (2) = 5.65, $p = .059$). A set of logistic regressions indicated that although there were no differences between those aged 6–7 and 8–12 (OR = 1.24, $p = .44$, [95% CI, .72–2.13] and those aged 8–12 and 13–15 (OR = 1.54, $p = .11$, [95% CI, .91–2.63], the willingness to share the YT video watched with *everyone* was significantly higher for those aged 13–15 (47.2%) than for those aged 6–7 (31.9%) (OR = 1.91, $p < .05$, [95% CI, 1.10–3.31]. Again, similar to motivation, this result may be due to overconfidence on the part of older youth in handling online safety themselves and through their network of friends.

Effects of Parental Restrictions on YouTube

Before the children/teens watched the YouTube video, they were asked if their parents restricted what they watched on YouTube. Although not predicted, we sought to examine if this measure would interact with the age categories in its effect on online safety beliefs and the perceived importance of restricting the sharing of the YouTube video watched. In the case of children/teens saying that their parents restricted what they watched on YouTube, there was an overall effect of age ($F = 3.90, p < .05$), with SNK contrasts revealing that the teens aged 13–15 (M = 6.05; SD = 1.03) had significantly more favorable online safety beliefs than the children aged 6–7 (M = 5.53; SD = 1.24; $p < .05$). There were no differences for the teens aged 13–15 versus the children aged 8–12 (M = 5.77; SD = 1.27) or among the age categories in the case of parents *not* restricting what their children watched on YouTube. (In the latter case, the children aged 6–7 had more favorable online safety beliefs, but these were not significant versus other age categories.)

A similar pattern emerged for the importance of restricting sharing of the YouTube video watched. For children/teens indicating that their parents restricted what they watched on YouTube, there was an effect of age ($F = 2.76, p < .10$), with SNK contrasts revealing that the teens aged 13–15 (M = 5.29; SD = 2.08) placed significantly greater importance on restricting the sharing of the YouTube video they watched than the children aged 6–7 (M = 4.55; SD = 2.19; $p < .10$). There were no differences for teens aged 13–15 versus children age 8–12 (M = 4.82; SD = 2.06) or among the age categories in the case of parents who did *not* restrict what their children watched on YouTube. Again, in the latter case, the children aged 6–7 placed greater importance on restricting the YouTube video they watched, but this was not significant versus other age categories. Overall, it appears that the oldest age category (i.e., the strategic age group, those teens aged 13–15) can be (positively) affected by perceived parental restrictions that have an impact on teens' online safety beliefs and the importance of restricting the sharing of online videos watched.

Discussion

Overall, our results suggest that it is possible to empower children to protect what information (e.g., videos) they share on social media sites such as You Tube. Our findings depend on the type of cognitive defense strategy employed (quiz with feedback, educational video, or absence of a strategy), the age group of the child (strategic, cued, and limited), their motivation to restrict sharing in general, and perceived parental restrictions on viewing. We now summarize and discuss our key findings.

Online Safety Beliefs

Based on the cognitive defense strategies we tested experimentally, (1) the quiz with feedback was more effective than the educational video and (2) the video was better than the control in influencing online safety beliefs. The strategic age group (aged 13–15) was more likely than the cued age group (aged 8–12) to have a more favorable change in their online safety beliefs for greater protection. We also found that those children with a higher motivation to restrict sharing (in general) had a more favorable change in their online safety beliefs than those with a lower motivation to restrict sharing (in general).

Sharing Decisions

Our results indicate that the quiz with feedback and educational video conditions were significantly better in restricting sharing than the control condition. This is important given the relatively high percentage of children/teens willing to share the YouTube video they watched, ranging from 72% (video) to 75% (quiz) to 84% (control). The video was better than the quiz when the children chose to restrict the *audience* for sharing, with more in the quiz (44.8%) selecting "with everyone" compared to the video (30.0%). We believe that the importance of setting audience boundary restrictions when sharing was communicated more vividly with the video depiction of mice taking and storing the child's cookie crumbs (an analogy to their online information) compared to the quiz with feedback.

Also, it appears that some *overconfidence* was displayed by those who agree with the importance of restricting sharing and for the older children/teens (aged 13–15) that had a greater willingness to share the video with everyone. For this strategic age category, it may be that their experience with digital devices and online access to information has fostered a greater focus, learning, and retention of the relevance of privacy issues (Maccoby and Hagen 1965). Such improvement in one's ability to understand and process key information is an important precursor to persuasion (Petty and Cacioppo 1986). As noted above, this finding also may be a result of overconfidence on the part of motivated and/or older youth in handling online safety themselves and through their network of friends. So, even though the quiz and video were effective in enabling protective cognitive defenses (i.e., setting boundaries on sharing), there is still ample room for development and improvement in the type and utilization of strategies employed.

Parental Restrictions

Our results indicate that perceived parental monitoring of children's online use can be helpful in some situations. For example, the child's/teen's perception of their parents restricting their YouTube viewing positively affected their online safety beliefs and the importance of restricting videos shared for the strategic age group (aged 13–15) versus the limited age group (aged 6–7). Such perception of parental monitoring of online behaviors may help over time, with such monitoring operating as a shared learning experience as opposed to a fear of punishment on behalf of children and teens.

Policy Implications

Our study aids regulatory and self-regulatory efforts for enhancing children's digital literacy and their cognitive defenses in setting boundaries for what they share online. In a broader sense, this includes efforts to empower children to restrict access to their personal information. For many years, federal (e.g., FTC), state (e.g., California), and self-regulatory agencies (e.g., Advertising Self-Regulatory Council's CARU), as well as companies that have websites and provide online services, have struggled with efforts to protect children and their personal information online. Even as COPPA celebrates 20 years of existence, challenges with ensuring verifiable parental consent and keeping up with emerging technology continue to exist. The FTC's goals of not only COPPA enforcement, but also encouraging self-regulatory efforts with industry to "streamline COPPA compliance," has led to a six-step plan for several approved Safe Harbor Programs (Magee 2018). The overall purpose of this FTC-driven plan is to guide companies through the process of protecting children online (Magee 2018). However, these efforts still focus on parental consent and protecting/controlling the access to information gathered by companies about and from children online. Our findings indicate that using cognitive defense strategies, such as a simple quiz with feedback or an educational video, can help empower children to protect *themselves* online.

In our study, we examined whether digital literacy knowledge was important for online safety and found that the quiz (with elaborated feedback) was more helpful for positively affecting children's and teens' online safety beliefs. With this in mind, federal agency privacy guidelines could be offered to nudge companies to expand online safety quizzes with feedback for children/teens to build their online safety/privacy knowledge and beliefs. Currently, a self-regulatory effort among leading advertising organizations ("Privacy for America") is focusing on data protection solutions, but it is not yet addressing children's privacy knowledge specifically at this point (AAAA 2019).

When sharing decisions were the focus, especially regarding restricting the sharing audience, the educational video was more useful. Thus, guidelines also could promote the use of online privacy videos aimed at children's/teens' online decision making (e.g., https://www.youthprivacyprotection.org funded by the Digital Trust Foundation). Importantly, such videos should be accessible at the same point at which children/teens consider sharing personal information online (e.g., within an app on a smartphone). However, it should be noted that both the quiz and video were better than the control condition (in which no cognitive defense strategy was provided) in improving knowledge and decision making. Also, such expansion efforts with quizzes and videos should be tested using a sample of children/teens. Other direct educational efforts could be made through the FTC's consumer website (https://www.consumer.ftc.gov/topics/protecting-kids-online), its annual Privacy Con, and its Division of Privacy & Identity Protection. Similar educational efforts at nonprofits (e.g., Electronic Privacy Information Center) could help children's and teen's online privacy knowledge and decision making.

Certainly, over the past several years, there have been many important and well-funded educational campaigns at the federal level aimed at adolescents (e.g., the FDA's The Real Cost Campaign, the National Youth Anti-Drug Media Campaign). However, to our knowledge, such national campaigns do not yet exist for online privacy safety and are desperately needed. This is especially the case considering recent and significant COPPA violations (FTC 2019; U.S. v. Muscial.ly and Musical.ly, Inc. 2019; U.S. and the Attorney General of the State of NY v. Google LLC and YouTube LLC 2019). Considering the Google YouTube decision, one dissenting FTC commissioner argued for a technological "backstop" solution whereby YouTube algorithms would help identify child-oriented content upfront and prevent behavioral advertising, rather than relying on the self-identification by YouTube channel creators outlined in the settlement (Slaughter 2019). However, given the millions of YouTube child channels, such a promising technological approach might be best combined with enhancing children and teens' cognitive defense education *before* such encounters arise.

Our study also suggests slightly different (and positive) effects of cognitive defense education depending on whether such knowledge and/or sharing decisions are important. However, there is no doubt that challenges remain, as overconfidence seems to accrue with increases in one's motivation to restrict their sharing and especially with age. On a positive note, perceived parental involvement and cognitive defense strategies can have an impact even for the oldest, strategic youth categories. Thus, a combination of educational defense strategies similar to those tested in the current study, along with an active role by parents, may be helpful in empowering children and teens to internalize online safety beliefs, be more judicious, and utilize active privacy protective strategies when sharing their information online.

Future Research

Because our study focused solely on enhancing children's and teens' *ability* (empowering them) to protect their information online through cognitive defense strategies, as well as accounting for *motivation* to restrict their sharing according to different

age categories (strategic, cued, and limited), there are many other areas of research that are warranted. For example, children's and teen's *opportunity* to restrict/share information online could be studied by varying the amount of time it takes to read privacy policies, or by studying the effects of whether children/teens are free/not free from distractions (e.g., friends' encouragement to share information; pressuring app downloads). Paying attention to such details that might affect restricting access should be considered as part of digital literacy efforts by federal, state, and self-regulatory agencies.

In addition, the endurance of the online safety beliefs could be tested longitudinally based on different degrees of motivation or ability to restrict information. No doubt, different types of educational quiz and video approaches and more tailored age measures for children/teens could be studied in the future. Also, would older teens (e.g., aged 16–18) respond in the same fashion as the younger age groups? Other individual characteristics for children/teens could be examined, such as gender effects in online risk taking. For example, will male youth be more inclined to take risks online regarding their private information than female youth? In addition, as noted previously, there is a real need to develop a national education campaign to enhance and empower children and teens to protect their online privacy. Also, would external or peripheral cues (e.g., social media influencers) be effective in influencing online safety beliefs and decisions to restrict online information sharing? In addition, although some efforts have been made to develop general digital literacy scales (cf. Trepte et al. 2015), work is needed on measures of digital literacy for youth. Another research avenue may deal with how to address overconfidence in online privacy protection, especially for those who might be over-reliant on their motivation, abilities, network of friends, and/or parents to handle their privacy protection. Finally, convenient access to websites, platforms, and applications by children (not just sites focused on children or advertising to children) must be addressed to understand how to encourage active protection strategies and parental monitoring behaviors. For example, will such cognitive defenses and digital literacy work in the context of popular gaming app chat rooms (Jargon 2019)? Such research would be welcomed in helping to rebalance information power for children and teens online, and to empower children to internalize the importance of online safety and actively restricting what they share online.

Appendix A

"Tips for Online Safety" Quiz

Please answer the following questions by marking either "true" or "false" to the best of your knowledge about online safety issues.

1. **True or False? Every time you go online, a part of yourself is left behind.**

   True
   False
   Don't Know

   Response if correct: Correct! It is TRUE that every time you go online, a part of yourself is left behind.

   Response if incorrect: Sorry, but you got this one wrong. It is actually TRUE that every time you go online, a part of yourself is left behind.

   The correct answer is TRUE. Every time you go online, a part of yourself is left behind.

2. **True or False? Your posts, likes, and shares will go away—they never stick.**

   True
   False
   Don't Know

   Response if correct: Correct! It is FALSE that your posts, likes, and shares will go away - they never stick.

   Response if incorrect: Sorry, but you got this one wrong. It is actually FALSE because your posts, likes, and shares DO NOT go away - they DO stick.

   The correct answer is FALSE. Your posts, likes, and shares DO NOT go away they DO stick.

3. **True or False? Third-party shadows follow wherever you click.**

   True
   False
   Don't Know

   Response if correct: Correct! It is TRUE that third-party shadows follow wherever you click.

   Response if incorrect: Sorry, but you got this one wrong. It is actually TRUE that third-party shadows follow wherever you click.

   The correct answer is TRUE. Third-party shadows follow wherever you click.

4. **True or False? When you log onto a website, that company never shares your information with third parties through secret communication.**

   True
   False
   Don't Know

   Response if correct: Correct! It is FALSE that when you log onto a website, that company never shares your information with third parties through secret communication.

   Response if incorrect: Sorry, but you got this one wrong. It is actually FALSE because when you log on to a website, that company sometimes DOES share your information with third parties through secret communication.

   The correct answer is FALSE. When you log onto a website, that company sometimes DOES share your information with third parties through secret communication.

5. True or False? Third parties are companies that take your online information and share it with other companies often for money.

True
False
Don't Know

Response if correct: Correct! It is TRUE that third parties are companies that take your online information and share it with other companies often for money.

Response if incorrect: Sorry, but you got this one wrong. It is actually TRUE that third parties are companies that take your online information and share it with other companies often for money.

The correct answer is TRUE. Third parties are companies that take your online information and share it with other companies often for money.

6. True or False? As you give away personal information, these companies send you ads that you may or may not wish to see.

True
False
Don't Know

Response if correct: Correct! It is TRUE that as you give away personal information, these companies send you ads that you may or may not wish to see.

Response if incorrect: Sorry, but you got this one wrong. It is actually TRUE that as you give away personal information, these companies send you ads that you may or may not wish to see.

The correct answer is TRUE. As you give away personal information, these companies send you ads that you may or may not wish to see.

7. True or False? Giving companies and third parties your personal information will help your online experience be as secure as it can be.

True
False
Don't Know

Response if correct: Correct! It is FALSE that giving companies and third parties your personal information will help your online experience be as secure as it can be.

Response if incorrect: Sorry, but you got this one wrong. It is actually FALSE because giving companies and third parties your personal information will actually REDUCE the security of your online experience.

The answer is FALSE. Giving companies and third parties your personal information will actually REDUCE the security of your online experience.

Great job! You completed the quiz. Now we just want to ask you a few questions about the quiz you just took.

Editorial Team

M. Paula Fitzgerald served as guest editor and Sterling Bone served as associate editor for this article.

Declaration of Conflicting Interests

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

Funding

This research study was funded internally by one of the authors' academic institutions.

References

American Association of Advertising Agencies (2019), "New 'Privacy for America' Coalition Calls for Strong Data Privacy Protections for All Americans," (April 8), https://www.aaaa.org/new-privacy-for-america-coalition-calls-for-strong-data-privacy-protections-for-all-americans/.

Anderson, Monica (2019), "How Parents Feel About—and Manage—Their Teens' Online Behavior and Screen Time," *Pew Research Center* (March 22), https://www.pewresearch.org/fact-tank/2019/03/22/how-parents-feel-about-and-manage-their-teens-online-behavior-and-screen-time.

Andrews, J. Craig (1987), "Motivation, Ability, and Opportunity to Process Information: Conceptual and Experimental Manipulation Issues," in *Advances in Consumer Research*, Vol. 15, M. J. Houston, ed. Provo, UT: Association for Consumer Research, 219–25.

Andrews, J. Craig and Richard G. Netemeyer (2015), "The Role of Social Marketing in Preventing and Reducing Substance Abuse," in *Handbook of Persuasion and Social Marketing*, Vol. 3, Chap. 6, David Stewart, ed. New York: Praeger, 155–94.

Andrews, J. Craig and Terence A. Shimp (1990), "Effects of Involvement, Argument Strength, and Source Characteristics on Central and Peripheral Processing of Advertising," *Psychology & Marketing*, 7 (3), 195–214.

Andrews, J. Craig and Terence A. Shimp (2018), *Advertising, Promotion and Other Aspects of Integrated Marketing Communications*, 10th ed. Boston: Cengage.

Batra, Rajeev and Michael L. Ray (1986), "Situational Effects of Advertising Repetition: The Moderating Influence of Motivation, Ability, and Opportunity to Respond," *Journal of Consumer Research*, 12 (4), 432–45.

Brehm, Sharon S. and Jack Williams Brehm (1981), *Psychological Reactance: A Theory of Freedom and Control*. New York: Academic Press.

Brucks, Merrie, Gary M. Armstrong, and Marvin E. Goldberg (1988), "Children's Use of Cognitive Defenses Against Television Advertising: A Cognitive Response Approach," *Journal of Consumer Research*, 14 (4), 471–82.

Children's Advertising Review Unit (CARU) (1997), *Self-Regulatory Guides for Children's Advertising*. New York: Council of Better Business Bureaus, 1–11.

Children's Online Privacy Protection Act (COPPA) (1998), Pub. Law No. 105-277, 112 Stat. 2681-2781 (codified at 15 U.S.C.

6501-6506 (October 21), http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

Cohen, Jacob (1969), *Statistical Power Analysis for the Behavioral Sciences*. New York: Academic Press.

Common Sense Media (2018), "How Kid-Friendly is the YouTube Kids App?" (accessed October 25, 2019), https://www.commonsensemedia.org/youtube/how-kid-friendly-is-the-youtube-kids-app.

Egelman, Serge (2017), "We Tested Apps for Children. Half Failed to Protect their Data," *The Washington Post* (July 27), https://www.washingtonpost.com/news/the-switch/wp/2017/07/27/we-tested-apps-for-children-half-failed-to-protect-their-data/?utm_term=.f43eb57709a1.

Federal Trade Commission (1997), *Transcripts from the FTC's Public Workshop on Consumer Information Privacy*, Washington, D.C., June 10–13, https://www.ftc.gov/news-events/press-releases/1997/06/ftc-privacy-week-june-10-13.

Federal Trade Commission (1998), "*Children's Online Privacy Protection Rule (with updates),"* (accessed October 25, 2019), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

Federal Trade Commission (2016), "*Putting Disclosures to the Test (Workshop)*," (September 16), https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

Federal Trade Commission (2019), "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law," (September 4), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

Friestad, Marian and Peter Wright (1994), "The Persuasion Knowledge Model: How People Cope with Persuasion Attempts," *Journal of Consumer Research*, 21 (1), 1–31.

Gregan-Paxton, Jennifer and Deborah Roedder John (1997), "The Emergence of Adaptive Decision Making in Children," *Journal of Consumer Research*, 24 (1), 43–56.

Hobbs, Renee (2011), *Digital and Media Literacy: Connecting Culture and Classroom*. Thousand Oaks, CA: Corwin Press.

Hoy, Mariea Grubbs and J. Craig Andrews (2004), "Adherence of Prime-Time Television Advertising Disclosures to the 'Clear and Conspicuous Standard': 1990 Versus 2002," *Journal of Public Policy & Marketing*, 23 (2), 170–82.

Interactive Advertising Bureau (2015), "IAB Code of Conduct," (accessed October 25, 2019), https://www.iab.com/wp-content/uploads/2015/06/IAB_Code_of_Conduct_10282-21.pdf.

Jargon, Julie (2019), "The Dark Side of Discord, Your Teen's Favorite Chat App," *The Wall Street Journal* (June 11), https://www.wsj.com/articles/discord-where-teens-rule-and-parents-fear-to-tread-11560245402.

John, Deborah Roedder (1999), "Consumer Socialization of Children: A Retrospective Look at Twenty-Five Years of Research," *Journal of Consumer Research*, 26 (3), 183–213.

Kelman, Herbert C. (1961), "Processes of Opinion Change," *Public Opinion Quarterly*, 25 (1), 57–78.

Maccoby, Eleanor and John W. Hagen (1965), "Effects of Distraction upon Central Versus Incidental Recall: Developmental Trends," *Journal of Experimental Child Psychology*, 2 (3), 280–89.

MacInnis, Deborah J., Christine Moorman, and Bernard J. Jaworski (1991), "Enhancing and Measuring Consumers' Motivation, Ability, and Opportunity to Process Brand Information from Advertisements," *Journal of Marketing* 55 (4), 32–53.

Magee, Peder (2018), "Happy 20th Birthday, COPPA," *Federal Trade Commission Business Blog* (October 22), https://www.ftc.gov/news-events/blogs/business-blog/2018/10/happy-20th-birthday-coppa.

McAfee (2014), "Cyberbullying Triples According to New McAfee 2014 Teens and the Screen Study," (accessed January 2019), *McAfee 2014 Teens and Screen Study* (June 3), https://mcafee-dr.mcafee.com/us/about/news/2014/q2/20140603-01.aspx.

Ofcom (2017), "Children and Parents: Media Use and Attitudes Report," (November 29), https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf, 1–303.

Paivio, Allan (1969), "Mental Imagery in Associative Learning and Memory," *Psychological Review*, 76 (3), 241–63.

Pechmann, Cornelia and Susan J. Knight (2002), "An Experimental Investigation of the Joint Effects of Advertising and Peers on Adolescents' Beliefs and Intentions About Cigarette Consumption," *Journal of Consumer Research*, 29 (1), 5–19.

Pechmann, Cornelia, Linda Levine, Sandra Loughlin, and Frances Leslie (2005), "Impulsive and Self-Conscious: Adolescents' Vulnerability to Advertising and Promotion," *Journal of Public Policy & Marketing*, 24 (2), 202–21.

Petty, Richard E. and John T. Cacioppo (1986), *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer-Verlag.

Pew Research Center (2018), "Teens, Social Media & Technology 2018," (May 31), http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/.

Pickhardt, Carl E. (2009), "Rebel with a Cause: Rebellion in Adolescence," *Psychology Today* (December 6), https://www.psychologytoday.com/us/blog/surviving-your-childs-adolescence/200912/rebel-cause-rebellion-in-adolescence.

Pollay, Richard W., S. Siddarth, Michael Siegel, Anne Haddix, Robert K. Merritt, Gary A. Giovino, et al. (1996), "The Last Straw? Cigarette Advertising and Realized Market Shares Among Youth and Adults, 1979–1993," *Journal of Marketing*, 60 (2), 1–16.

Roedder, Deborah L. (1981), "Age Differences in Children's Responses to Television Advertising: An Information Processing Approach," *Journal of Consumer Research*, 8 (2), 144–53.

Rossiter, John R. and Thomas S. Robertson (1974), "Children's TV Commercials: Testing the Defenses," *Journal of Communication*, 24 (4), 137–44.

Rozendaal, Esther, Moniek Buijzen, and Patti Valkenburg (2009), "Do Children's Cognitive Advertising Defenses Reduce Their Desire for Advertised Products?" *Communications*, 34 (3), 287–303.

Schwarz, Norbert (2004), "Meta-Cognitive Experiences in Consumer Judgment and Decision Making," *Journal of Consumer Psychology*, 14 (4), 332–48.

Shu, Catherine (2018), "YouTube Releases Its First Report About How It Handles Flagged Videos and Policy Violations," (April 23), https://techcrunch.com/2018/04/23/youtube-releases-its-

first-report-about-how-it-handles-flagged-videos-and-policy-violations/.

Slaughter, Rebecca Kelly (2019), "*Dissenting Statement of Commissioner Rebecca Kelly Slaughter in the Matter of Google LLC and YouTube, LLC,"* Federal Trade Commission (September 4), https://www.ftc.gov/system/files/documents/public_statements/1542971/slaughter_google_youtube_statement.pdf.

Steinberg, Laurence D. (2020), *Adolescence* (12th ed). New York: McGraw-Hill.

Steinberg, Laurence D. and Elizabeth S. Scott (2003), "Less Guilty by Reason of Adolescence: Development Immaturity, Diminished Responsibility, and the Juvenile Death Penalty," *American Psychologist*, 58 (12), 1009–18.

Trepte, Sabine, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhofer, et al. (2015), "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)," in *Reforming European Data Protection Law*, Chap. 14, Serge Gutwirth, Ronald Leenes and Pau de Hert, eds. Law, Governance, and Technology Series 20, DOI:10.1007/978-94-017-9385-8__14.

U.S. and the Attorney General of the State of New York v. Google LLC and YouTube, LLC (2019), Case No. 1:19-cv-02642, U.S. District Court, District of Columbia, September 4, 1–31.

U.S. v. MUSICAL.LY and MUSICAL.LY, INC. (2019), Case No. 2: 19-cv-1439, U.S. District Court, Central District of California, February 27, 1–25.

Van der Kleij, Fabienne M., Remco C. W. Feskens, and Theo J. H. M. Eggen (2015), "Effects of Feedback in a Computer-Based Learning Environment on Students' Learning Outcomes: A Meta-Analysis," *Review of Educational Research*, 85 (4), 475–511.

Walker, Kristen L. (2016), "Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection," *Journal of Public Policy & Marketing*, 35 (1), 144–58.

Walker, Kristen L., Tina Kiesler, and Summer Malone (2016), "Youth-Driven Information Privacy Education Campaign 2015–16," Digital Trust Foundation, Grant Report (accessed October 25, 2019), http://hdl.handle.net/10211.3/178689.

Wendling, Mike (2017), "YouTube Child Protection 'Failing,'" *BBC Trending* (August 5), http://www.bbc.com/news/blogs-trending-40808177.

White, Claire M., Michaela Gummerum, and Yaniv Hanoch (2015), "Adolescents' and Young Adults' Online Risk Taking: The Role of Gist and Verbatim Representations," *Risk Analysis* 35 (8), 1407–22.