What kinds of personal data do primary school pupils share with whom? Children's view of personal data and its implications for teaching about privacy

Martin Hermida

Schwyz University of Teacher Education, Switzerland

Raffael Meier

Schwyz University of Teacher Education, Switzerland

Iwan Schrackmann

Schwyz University of Teacher Education, Switzerland

Nina Imlig-Iten

Schwyz University of Teacher Education, Switzerland

Eva Marinus

Schwyz University of Teacher Education, Switzerland

ABSTRACT

Safeguarding personal digital data is crucial and requires appropriate training. However, privacy remains a novel topic, leaving teachers with limited guidance. This study investigates how elementary school students perceive personal data and assesses pre-service teachers' accuracy in predicting children's responses. Employing Nissenbaum's contextual integrity framework, the outcomes of this research offer a nuanced perspective on privacy, considering different recipients and data types. The study surveyed 94 Grade 3 and Grade 5 students, asking them to indicate with which recipients (no one, parents, best friends, class, all other people) they would share specific information. In addition, 75 pre-service teachers were asked to indicate what they expected Grade 5 children would share with whom. The findings show: 1. what information Grade 3 and Grade 5 students consider to be most private, 2. which recipients they trust the most, 3. varying sharing practices between Grade 3 and 5, and 4. a tendency for pre-service teachers to underestimate children's privacy sharing behavior. In the discussion section we propose five recommendations for enhancing digital privacy education.

Keywords: *privacy, media education, media literacy, pedagogical content knowledge, data protection.*

INTRODUCTION

With the rise of digital media, controlling the flow of one's personal information has become challenging. Users not only need to monitor which personal information is flowing to others, but also which information is shared with and automatically collected by companies providing devices (e.g., smartphones) and services (e.g., social networks). Around 80% of adults believe they have little to no control over the personal data companies collect and are concerned about how companies use that data (Pew Research Center, 2019). Also, most users are worried that their personal data is not safe (Symantec, 2015). Despite their concerns about their personal data, users seldomly act to protect it, which has become known as the 'privacy paradox' (Barnes, 2006; Kokolakis, 2017). Until now, most of the research about data privacy has focused on adults. However, over the last decades, children have also become avid users of digital technologies and researchers have started to investigate their understanding of different computer science concepts, such as the Internet (Babari et al., 2023; Papastergiou, 2005) and data security and privacy (Chaudron et al., 2017; Hermida, 2019; Kodama et al., 2017; Kumar et al, 2017; Livingstone et al., 2019; Papastergiou, 2005; Zhang-Kennedy et al., 2016; Zhao et al., 2019;).

Studies show that children under the age of 6 usually have low risk awareness and low understanding that sharing information online can involve privacy risks (Bakó, 2016). However, from 6 years onwards, children seem to be able to identify certain privacy risks and threats, particularly over-sharing personal information online and revealing their real identity (Zhao et al., 2019). Kumar et al. (2017) found in their study with 26 children aged 5 to 11 that they can differentiate between different actors and different types of information on the topic of privacy. They argue that strengthening children's privacy literacy is not about teaching rules, but about helping them establish appropriate information flow. Zhang-Kennedy et al. (2016) describe that for children between 7 and 11 years old, privacy consists of four models: a) being alone, b) having secret or special things (e.g., passwords, diary), c) keeping information to themselves and not regretting disclosing it, and d) not talking to strangers or suspicious people, and that the main threats to these understandings of privacy are peers, mean strangers, parents, and bad media (e.g., inappropriate content). In addition, Livingstone et al. (2019) confirmed that children begin to form concepts about private data, online privacy, and data protection around age 8. Finally, in the international Global Kids Online study, clear age trends were observed: in particular, younger children (ages 9-11) showed less competence in managing their online privacy settings than adolescents (ages 12-17) (Byrne et al., 2016).

Our goal is to contribute to this field of research by investigating children's sharing practices of personal information with different recipients. The results of this study will inform what kind of information is particularly precious for children and will therefore provide concrete topics that can be used to teach about privacy in school.

Regulation vs. empowerment via teaching

In the European Union and in the United States of America there are special regulations to protect children from sharing too much data and to prevent companies from collecting too much data about them (COPA - Children's Online Privacy Protection Act; GDPR - General Data Protection Regulation). However, service providers do not strictly enforce such regulations. They often use declarative age restrictions to exclude children below the age of 13 from their services (Finnegan, 2020). This does not seem to be effective as still more than a quarter of 9-to-11-year-olds in Europe report using social networks on a daily basis (Smahel et al., 2020).

Without effective regulations in place the best way to help children protect their privacy is to teach them about privacy. The European Union has formulated the "European Framework for the Digital Competence of Educators" which states which aspects of digital literacy children should acquire. One learning goal is to effectively manage the data they produce through digital technologies and services (Redecker, 2017). In Switzerland, where this study was conducted, the national curriculum for primary schools suggests that children should be taught about 1) possible consequences of sharing data on social media, 2) the ways service providers make money (e.g., by selling user data) and 3) what kind of personal data might be sensitive (D-EDK, 2016).

Effective education not only increases knowledge and skills, it also increases self-efficacy (Schunk, 1995). For example, research has shown that users' beliefs in their ability (self-efficacy) to protect their data will increase their use of data protection strategies (Adhikari & Panda, 2018; Hermida et al., 2022; Hichang, 2010; Meier et al., 2022). These findings support the idea that

adequate education is the pathway towards increasing users' ability to protect their privacy.

Media literacy education: Teaching about privacy

On the education policy level, society wants to foster privacy protection via adequate teaching. This requires effective teaching practices in schools. Knowledge about how to best teach a certain topic to a certain age or target group is also known as pedagogical content knowledge (PCK). It comprises the knowledge of representing a subject in a way that others can understand it (Shulman, 1986), which in turn should improve learning outcomes. For example, from research in mathematics we know that a teacher with high PCK will be more likely to positively influence students' knowledge growth than a teacher with low PCK (Baumert & Kunter, 2013; Hill et al., 2005). One aspect of pedagogical content knowledge is being aware of the levels of understanding the learners have and what kind of (pre)conceptions they hold about a topic (see also the model of didactic reconstruction, Diethelm et al., 2012; Duit, 2007; Kattmann et al., 1997;). Such knowledge helps in designing appropriate lesson plans and optimizing instruction accordingly (e.g., in physics: Edelsbrunner et al., 2018; Schneider & Hardy, 2013). Thus, in the context of teaching about privacy, it can be assumed that teachers who know how children perceive privacy and personal data will also have a head start in effectively teaching the subject.

Usually teaching children about privacy typically involves imprinting several rules - for example *do not share your phone number online*. However, research findings suggest that while children may rely on such explicit rules, they do not understand the underlying privacy norms (Kumar et al., 2017). Furthermore, to our knowledge, there is no research regarding pre-service or in-service teachers' understanding of their pupils' conception and application of privacy. In contrast, most studies in this area have focused on teacher's perception of the ability of their (future) students to use digital technologies, showing that teachers typically overestimate the digital skills of their students (Dong & Mertala, 2021; Mertala, 2020).

In this study we want to gain first insights into privacy perceptions in primary school children and to find out how well pre-service teachers can predict their future pupils' behavior. In the next two sections, we will demonstrate that children already gain considerable experience managing their privacy in their non-digital lives and that this everyday life experience will and

should form the basis to teach them about privacy in digital media.

Definition of privacy and the contextual integrity framework

Teaching and learning about privacy are complicated by the lack of a standardized definition of privacy. Today's general conception of privacy is based on the definition of Warren and Brandeis (1890), who refer to it as *the right to be left alone*. Although numerous attempts have been made to clarify the concept, no universal definition of privacy could be established (Lukács, 2016). This is probably because its concrete form and meaning differ depending on societal characteristics and the economic and cultural paradigms that surround it. Moreover, the meaning and applicability of privacy depend on the situation, on what kind of information is shared in what form and, importantly, with whom. The contextual integrity framework (Nissenbaum, 2010) takes these dependencies into account. It focuses on the exchange of information within specific contexts and under specific norms. Moreover, it accounts for the various situations in which different kinds of information are exchanged and therefore it allows for varying expectations regarding privacy by the parties involved. Focusing on the flow of information, the framework allows for a precise description of situations in which personal data is exchanged.

According to the contextual integrity framework the exchange of information is characterized by four elements: 1) the context, 2) the sender and the recipient, 3) the kind of information and 4) the transmission principles. Being able to control one's privacy therefore means being able to control the flow of one's personal information in different contexts. Privacy (contextual integrity) is preserved when the informational norms in a given situation are respected and breached when they are violated. As an example, we can look at the casual chatter among a large group of pupils during a school break (context). One pupil (sender) may tell the other classmates (recipients) that her favorite color is blue (type of information). The flow of the information in this particular context is shaped by the transmission principles of this specific context involving this specific sender and these recipients. It is for example to be expected that the pupil sharing her favorite color did so voluntarily, that there is no need for the recipients to keep the information confidential and that there will be no transcript of the conversation. Now imagine a

different situation where the same pupil (sender) sends a chat message about who her crush is (type of information) to her best friend (recipient). In this case, the information flows to a different recipient (just that one best friend), it is a different kind of information (intimate private life) and a conversation among best friends is based on different transmission principles (some of the information is expected to be confidential). We can clearly picture the informational norms expected from the pupil sharing the information and predict when she would consider her privacy to be violated - for example when the recipient shares this information with others or when the chat service provider analyzes the message content for profiling purposes. Along with any change in the four elements involved the expectations regarding privacy of the party sharing the information will change, too. Hence, fundamental to protecting one's privacy is the power to stay in control of the flow of one's personal information.

Children's initial experiences with privacy and the transition to privacy in digital media use

Privacy is not only a normative value; it also fulfills an important function in personal development. When operationalized as time spent alone, privacy has increased for everyone over the last few decades (Anttila et al., 2020) and with age: the older children are, the more time they spend alone (Larson & Richards, 1991). The older adolescents get, the more they appreciate their privacy (Corsano et al., 2006). Research has shown that adolescents who could spend more time alone are psychologically better adapted than their peers with less privacy opportunities. This, in turn, has a positive influence on their individual development and the development of their autonomy and identity (Larson, 1990, Hipson et al., 2021; Thomas & Azmitia, 2019).

In addition to describing privacy as having the right to be left alone (Warren & Brandeis, 1890), children have referred to privacy as the possibility "to hide secrets or special things", "to keep things to yourself" and "to not talk to strangers" (Zhang-Kennedy et al., 2016, p. 392). Although such broad operationalizations and descriptions of privacy are difficult to translate into real world (digital) interactions, these results clearly demonstrate that the development and need for privacy enter children's lives long before they independently use digital media. Early in their lives children have no privacy with adults controlling their time and space (Wolfe, 1978). In preschool children must share a caregiver's attention with a group of other children. The

amount of supervision decreases again when children start to go to and return from school on their own and start to attend secondary school, which typically involves longer and more independent travel. In parallel, children become more and more independent during their spare time. Encounters with other people become more frequent, gradually including less familiar persons and strangers. These encounters offer children the opportunity to experience the consequences of sharing their personal information and what it means when they retain or lose control over it. For example, when someone else passes on their secrets, mocks them for an intimate piece of information or rewards shared information with sharing personal information as well.

Children's introduction to digital media follows a similar transition: they engage with an increasing number of apps, content and people online, while the caretakers' supervision decreases. The only difference seems to be that it typically happens more abruptly. When children start to use digital gadgets and services, they suddenly have the same scope for action and access as adults. They can communicate with almost everybody and share information with known and unknown people as well as with service providers. While many parents mediate their children's technology use, most parents do this by talking to their children about safety and risks. The use of technical controls, such as Family Link is less common (Smahel et al., 2020; Stoilova et al., 2024), probably because of the technical demands that come along with them (Nikken & Opree, 2018). Furthermore, it is usually not obvious what information digital services collect and share with whom.

In sum, children typically already gain considerable experience protecting and managing their privacy in their non-digital lives, which offers a promising starting point for teaching about privacy in relation to digital media. In this study, we aim to collect data that can be used to increase teachers' pedagogical content knowledge regarding privacy and correspondingly improve their teaching and its outcomes. To determine which types of information to include in our study, we analyzed the data categories of the EU General Data Protection Regulation (GDPR) and consulted a Grade 3 and a Grade 5 teacher who gave us feedback based upon their teaching experiences.

Research questions

Our first three research questions focus on children's perception of privacy towards different types of information and recipients: *What do Grade 3 and 5*

children regard as their most private and what as their least private information (e.g., name, date of birth, grades)? (RQ1)

According to the contextual integrity framework we expect different kinds of information to be shared with certain recipients but not with others. Partly based on the micro systems in Bronfenbrenner's Ecological Systems Model and the sphere theory of the German Federal Constitutional Court we differentiated between parents, best friends, the school class and the entire world (Bronfenbrenner, 1979; Nebel, 2020). This leads to our second research question: *Which recipients do children trust the most with which kind of information? (RQ2)*

Here we expect different patterns for the two Grades, in particular to what degree they share information with their friends. Research findings show that sharing secrets is an important indicator for friendships among children (Liberman & Shaw, 2018) and that children expect friendships to entail self-disclosure (Bigelow, 1977). Their demand for trustworthy behavior between friends increases between the ages of 6 to 11 (Kahn & Turiel, 1988). Our third research question is therefore: *Do 3rd and 5th graders differ in how much information they would share with their friends? (RQ3)*

Our final research question focuses on how well pre-service teachers can predict which data Grade 5 children would share with whom. Teachers who know how their students perceive personal information can use this information when teaching about digital privacy. Hence our fourth research question is: *How accurately do pre-service teachers predict which data 5th-graders would share with whom? (RQ4)*

METHODS PRIMARY SCHOOL CHILDREN

Participants

Participants were 50 children (26 boys, 24 girls) from three Grade 3 classrooms and 44 children (23 boys, 21 girls) from three Grade 5 classrooms from a primary school in Switzerland. All children that were present on the day of testing participated. Ages were not registered. However, in Switzerland, these are typically between 8 and 10 years in Grade 3 and between 10 and 12 years in Grade 5.

The parents received an information letter about the study and were requested to contact the researchers or the teacher if they had any questions or did not agree for their children to participate. No such requests were made.

Materials

To measure which recipients children would trust with what kind of information we adapted the 'red circles' exercise from Swiss media education teaching materials that are commonly used to make primary school children aware of who they share information with (e.g., Hartmann et al., 2019, p. 85). The materials consisted of two worksheets with five empty squares representing: 1. Me all alone, 2. Best friends, 3. Mother or father, 4. The whole class, and 5. All other people. Both score sheets also had a circle for items that were not applicable. An English translation of the sheet is shown in Figure 1. For the first score sheet the children were asked to allocate 23 items into the squares or circle, indicating that they would share that information with that person/group. The second score sheet had four lines printed in each square, allowing the children to fill out their own items. The data gathered from the first score sheet is reported hereafter.

Figure 1. *Worksheet*

Procedure

Testing took place during school hours during one 45-minute session, all on the same morning in March 2021. The six classes were tested separately by the second and final author, who were testing in parallel in two classrooms. The teachers were present during testing and helped with classroom management. To ensure consistency across sessions, instructions were given according to a protocol. Before giving the instructions, all children received the first worksheet (with squares and circle) and the list with 23 items. The first worksheet was also projected on a screen and after introducing themselves, the researcher explained the aims of the research and the workings of the worksheet.

It was also stressed that the research was anonymous, and it was carefully explained how the researchers would make sure that no one would find out who wrote what on which worksheet. After three practice items and the opportunity to ask questions, the researcher proceeded to read aloud the items, one-by-one, giving the children 30 seconds to fill out the score sheet for each item. After finishing the last item, the children were asked to put their worksheet in an envelope and to seal it. After the sealed envelopes were collected by the researcher the second worksheet was distributed.

METHODS PRESERVICE TEACHERS

Participants

About one month later all 83 Bachelor students who were enrolled in their third year studying for a Bachelor of Arts in primary school education (n = 64) or for a Bachelor of Arts in pre-primary and primary education (n = 19) at a teacher education university in Switzerland and who were present during the online media education lecture were invited to participate in the study. The median age of the students was 24 (SD = 4.24, Range 20-41, 85% between 21 and 28). As far as we are aware the students did not have any specific knowledge about data protection and privacy and how to teach this to children, as this was their first lecture on this topic. Participation in the study was voluntary. Students could opt out or mark their data as not to be used for research purposes without expecting negative consequences. Three students decided to do so. In addition, three more students did not take part at all and two more terminated the questionnaire without inserting any data. Therefore, the data of 75 students was analyzed.

Materials

The materials of the students differed from those of the children in three ways:
1. The students were asked to complete the first worksheet twice. Once from their own perspective and the second as they would expect 5th graders to fill it out. For this study only the data of the second worksheet was used.
2. The students were given a link to an online survey instead of using paper and pencil.

3. The presentation of the worksheets: For the first worksheet, the answers were presented item for item in multiple choice format ("please make a spontaneous decision for each line to whom you would tell this thing. Tick ALL columns that apply."). For the second worksheet, a large, empty text field for each category offered the opportunity to add further items.

Screenshots of the materials can be found on the Open Science Framework[1].

Procedure

Data collection took place mid-April 2021 during a 1,5-hour online lecture which was part of a media education unit on data protection and privacy. The lecture was given by the second author under supervision of the third and fourth authors. At the beginning of the lecture the concept of personal data and its relevance for elementary school children was explained. Next, the study was briefly introduced. The instructions were given verbally by the second author and presented on a slide and repeated in text in the online questionnaire. After completing the consent part of the study, the students were given 15 minutes to fill out the online questionnaire. To avoid priming the students, it was not mentioned up front that school children had already been surveyed. This was done after the students finished the questionnaire.

RESULTS

RQ1: What do Grade 3 and 5 children regard as their most private and what as their least private information (e.g., name, date of birth, grades)?

To establish which information children value as their most private, we counted how often an item was placed in the square "Me all alone" and in no other square. In table 1 the items are ranked based on the number of mentions by the participants. The *diary* was seen as the most private item: from our 94 respondents, 48 placed the diary in the field "me all alone" only and in no other field, meaning they wouldn't share it with anybody. *Who I was mean to* and *How I lied once* were other items children in 3rd as well as 5th grade don't want to share with anybody else.

Table 1. *Mentions and ranks of Information children would tell no one else*

All children			3rd graders			5th graders		
Item	*n*	*Rank*	*Item*	*n*	*Rank*	*Item*	*n*	*Rank*
My diary	48	1	My diary	28	1	My diary	20	1
Who I was mean to	39	2	Who I was mean to	27	2	Who I was mean to	12	2
How I lied once	37	3	How I lied once	26	3	How I lied once	11	3
Whether I wash hands after going to the toilet	25	4	Whether I wash hands after going to the toilet	14	4	Whether I wash hands after going to the toilet	11	3
Who I am a little in love with	21	5	Who I am a little in love with	11	5	Who I am a little in love with	10	4
My cell phone code	17	6	My cell phone code	8	6	Cell phone numbers of my parents	9	5
Cell phone numbers of my parents	16	7	Cell phone numbers of my parents	7	7	My cell phone code	9	5
My password for laptop/computer/tablet	13	8	My password for laptop/computer/tablet	6	8	My password for laptop/computer/tablet	7	6
Who I do not like at all	9	9	Who I do not like at all	6	8	Who I do not like at all	3	7
Videos where I can be seen	6	10	Videos where I can be seen	4	9	Videos where I can be seen	2	8
My diseases	6	10	My username/player name	4	9	That someone is mean to me	2	8
My username/player name	5	11	My diseases	4	9	My diseases	2	8
That someone is mean to me	4	12	My cell phone number	2	10	Photos of me	1	9
My cell phone number	2	13	That someone is mean to me	2	10	My username/player name	1	9
Photos of me	2	13	My gender	1	11	My e-mail address	1	9
sex	1	14	Photos of me	1	11			
Photo of my house	1	14	Photo of my house	1	11			
My address	1	14	My address	1	11			
My grades in school report	1	14	My grades in school report	1	11			
My e-mail address	1	14						

Note. *N* = 94, *n* = 50 for 3rd graders and *n* = 44 for 5th graders. Occurrences a child placed an item exclusively in the field "Me all alone" and in no other field.

The information children value as their least private are the items they would share with *all other people*. The more often an item was placed there, the more participants saw fit to openly share it. Table 2 shows the three items most often put in the *all other people* square. With decreasing frequency, the items *My gender* and *My name* were the ones children were most open about. Followed by *My date of birth* and *My grades in school report* for 3rd graders and *My name* for 5th graders.

There is a considerable difference between sharing an item with *all other people* and sharing it with parents, friends, or classmates. While the latter are people the children are in personal contact with, the square *all other people* is the only one including strangers. The items shown in table 3 are the ones children would share with any recipient they are in personal contact with but *not* with *all other people*. Unsurprisingly, none of the children wanted to share their diary with all other people. But interestingly, children also do not want to share pictures of themselves or videos of themselves with *all other people*. The amount of information children would not share with all other people is higher among 5th graders than among 3rd graders.

To answer research question 1, it is clear that children would value their diary, them being mean to someone and them having lied as the most private personal information. Their gender, name and country - as well as grades and date of birth for 3rd-graders - are the personal data children would see fit to share with a wider audience. While neither 3rd graders nor 5th graders had the desire to share pictures or videos of themselves with strangers (all other people), the amount of data children would not want to share with all other people is higher among 5th graders than among 3rd graders.

Table 2. *Number of mentions in the all other people square*

All children			3rd graders			5th graders		
Item	*n*	*%*	*Item*	*n*	*%*	*Item*	*n*	*%*
Gender	41	44	Gender	13	26	Gender	28	64
Name	23	25	Name	11	22	Country	15	34
Country	21	22	Date of birth/Grades	7	14	Name	12	27

Note. *N* = 94, *n* = 50 for 3rd graders and *n* = 44 for 5th graders.

Table 3. *Information none of the children would share with all other people*

All children	3rd graders	5th graders
My diary	My diary	My diary
Photos of me	Photos of me	Photos of me
Videos where I can be seen	Videos where I can be seen	Videos where I can be seen
My cell phone code	My cell phone code	My cell phone code
My password for laptop/computer/tablet	My password for laptop/computer/tablet	My password for computer/laptop/tablet
That someone is mean to me	That someone was mean to me	That someone was meant to me
Who I was mean to	Who I was mean to	Who I was mean to
		My cell phone number
		Cell phone numbers of my parents
		Photo of my house
		My address
		How I lied once
		Who I am a little in love with
		My grades in school report

Note. *N* = 94, *n* = 50 for 3rd graders and *n* = 44 for 5th graders.

RQ2: Which recipients do children trust the most with which kind of information?

Analysis. To test which recipients children trust more with which data, we first display how all the entries for a particular item were distributed across each of the recipient squares as a heatmap (Figure 2). The more children named an item in combination with a particular recipient, the darker red the corresponding field is colored. The fewer children named an item in combination with a particular recipient, the brighter yellow a field is colored. The absolute counts for each combination are indicated by the numbers inside the fields.

Findings. The first item *my date of birth* would relatively often be shared with best friends, parents and the school class. It would be much less often shared with no one (*me all alone*) or *all other people*. Item 9 *my diary* would mostly be kept to oneself (*me all alone*) and seldomly be shared with another type of recipient.

The heatmap reveals children would most often share their personal data with their best friends and parents. However, there are items for which they would have more trust in their parents and others for which they would have more trust in their friends. For example, on the one hand, they are more willing to share who their crush is and how they lied once with their best friends. On the other hand, they are more willing to share their cell phone passcode and the password to their computer with their parents. There is also information that they would tend to fully keep for themselves, such as their diary and, to a lesser extent, who they were being mean to.

Thus, our answer to research question 2 is that, in general, children put most trust in their parents and their best friends. Depending on the kind of information, trust might be higher for one of these two recipient groups.
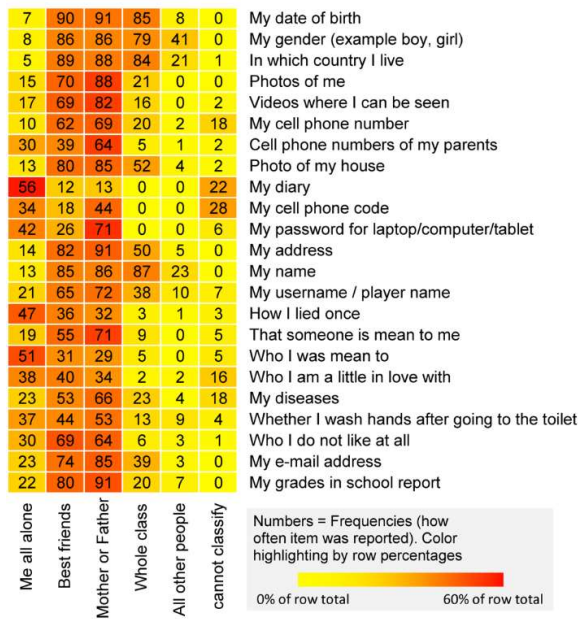
	Me all alone	Best friends	Mother or Father	Whole class	All other people	cannot classify	
My date of birth	7	90	91	85	8	0	
My gender (example boy, girl)	8	86	86	79	41	0	
In which country I live	5	89	88	84	21	1	
Photos of me	15	70	88	21	0	0	
Videos where I can be seen	17	69	82	16	0	2	
My cell phone number	10	62	69	20	2	18	
Cell phone numbers of my parents	30	39	64	5	1	2	
Photo of my house	13	80	85	52	4	2	
My diary	56	12	13	0	0	22	
My cell phone code	34	18	44	0	0	28	
My password for laptop/computer/tablet	42	26	71	0	0	6	
My address	14	82	91	50	5	0	
My name	13	85	86	87	23	0	
My username / player name	21	65	72	38	10	7	
How I lied once	47	36	32	3	1	3	
That someone is mean to me	19	55	71	9	0	5	
Who I was mean to	51	31	29	5	0	5	
Who I am a little in love with	38	40	34	2	2	16	
My diseases	23	53	66	23	4	18	
Whether I wash hands after going to the toilet	37	44	53	13	9	4	
Who I do not like at all	30	69	64	6	3	1	
My e-mail address	23	74	85	39	3	0	
My grades in school report	22	80	91	20	7	0	

Numbers = Frequencies (how often item was reported). Color highlighting by row percentages

0% of row total — 60% of row total

Figure 2. *Frequency with which an item was mentioned in combination with recipient (N = 94)*

RQ3: Do 3rd and 5th graders differ in how much information they would share with their friends?

Analysis. To determine whether there were differences between the answers of the 3rd and 5th graders, we first computed an exact Fisher test (Mehta & Patel, 1983) to obtain the significance of the differences for each pair of cells (3rd graders who chose the field/did not choose it, 5th graders who chose it/did not choose it). In a second step, we calculated the corresponding odds ratio as a coefficient of the effect size (Chinn, 2000), which we converted into the more common Cohen's d (Sanchez et al., 2023). Figure 3 shows for which cells and to what degree the groups differed from each other. The more an item would be shared with a particular recipient by 5th-graders than by 3rd-graders, the darker violet the field is colored. The more an item would be shared with a particular recipient by 3rd-graders than by 5th-graders, the darker green the field is colored.

Findings. In general, 5th graders would share considerably more items with their friends than 3rd graders. They would also share the aforementioned most private items (*Who I was mean to*, *How I lied once* and *My diary*) significantly more often with their best friends than 3rd graders. Regarding research question 3, it can be concluded that 5th graders are more likely to share personal data with their best friends than 3rd Graders. While sharing with friends is more common

among 5th-graders, the data in Table 3 show that 5th-graders also name more items they would not want to share with *all other people*.

So, the main difference between 3rd- and 5th-graders is that 5th-graders share more information with their friends but are also withholding more information from the general public.
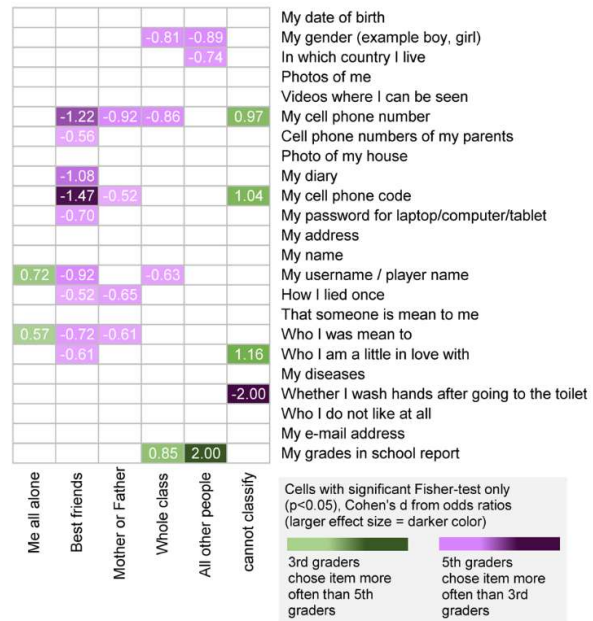

	Me all alone	Best friends	Mother or Father	Whole class	All other people	cannot classify	
My date of birth							
My gender (example boy, girl)				-0.81	-0.89		
In which country I live					-0.74		
Photos of me							
Videos where I can be seen							
My cell phone number		-1.22	-0.92	-0.86		0.97	
Cell phone numbers of my parents		-0.56					
Photo of my house							
My diary		-1.08					
My cell phone code		-1.47	-0.52			1.04	
My password for laptop/computer/tablet		-0.70					
My address							
My name							
My username / player name	0.72	-0.92		-0.63			
How I lied once		-0.52	-0.65				
That someone is mean to me							
Who I was mean to	0.57	-0.72	-0.61				
Who I am a little in love with		-0.61					
My diseases						1.16	
Whether I wash hands after going to the toilet					-2.00		
Who I do not like at all							
My e-mail address							
My grades in school report					0.85	2.00	

Cells with significant Fisher-test only (p<0.05), Cohen's d from odds ratios (larger effect size = darker color)

3rd graders chose item more often than 5th graders — 5th graders chose item more often than 3rd graders

Figure 3. *Shift between 3rd graders and 5th graders (Cohen's d from Odds Ratio & Exact Fisher-Test)*

RQ4: How accurately do pre-service teachers predict which data 5th-graders would share with whom?

Analysis. To test whether pre-service teachers' estimation of how their future pupils would fill out the assignment are accurate, we asked them to fill out the worksheet the way they would expect their future pupils to do. We then compared this data with the data from the children by computing an exact Fisher test (Mehta & Patel, 1983) for the corresponding odds ratio for each pair of cells (5th graders vs. pre-service teachers) as a coefficient of the effect size (Chinn, 2000) and converted it into Cohen's d (Sanchez et al., 2023).

Findings. Figure 4 shows where pre-service teachers under- and overestimated how their pupils would share a specific information. The more an item would be shared with a particular recipient by the children than was suggested by the pre-service teachers, the darker pink the corresponding field is colored. The less an item would be shared with a particular recipient by the children than was suggested by the pre-service teachers,

the darker blue the corresponding field is colored. The data shows that pre-service teachers overestimate the data children would share with *all other people* in several instances, especially their date of birth, pictures and videos of themselves or their address. On the other hand, they underestimate the trust children put in their parents (e.g. *passcodes, username*) as well as about their relationship with other pupils (e.g. *being mean*, *having a crush*, *not liking someone*). Most deviations between pupils and pre-service teachers were pre-service teachers underestimating the information children would share with their parents and overestimating the data children would share with *all other people*. And they occasionally underestimate what data children would share with their best friends as well, namely *diseases*, *washing hands after restroom* and their *grades*.

In sum, the answer to research question 4 is that pre-service teachers generally overestimate the amount of data children share with *all other people*. At the same time, they underestimate how much personal information pupils share with their parents and to some extent with their best friends.
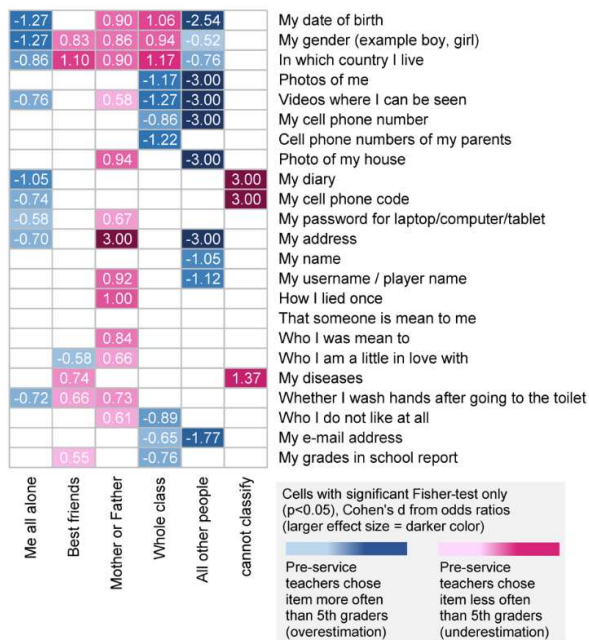

	Me all alone	Best friends	Mother or Father	Whole class	All other people	cannot classify	
	-1.27		0.90	1.06	-2.54		My date of birth
	-1.27	0.83	0.86	0.94	-0.52		My gender (example boy, girl)
	-0.86	1.10	0.90	1.17	-0.76		In which country I live
				-1.17	-3.00		Photos of me
	-0.76		0.58	-1.27	-3.00		Videos where I can be seen
				-0.86	-3.00		My cell phone number
				-1.22			Cell phone numbers of my parents
			0.94		-3.00		Photo of my house
	-1.05					3.00	My diary
	-0.74					3.00	My cell phone code
	-0.58		0.67				My password for laptop/computer/tablet
	-0.70		3.00		-3.00		My address
				-1.05			My name
			0.92		-1.12		My username / player name
			1.00				How I lied once
							That someone is mean to me
			0.84				Who I was mean to
		-0.58	0.66				Who I am a little in love with
		0.74				1.37	My diseases
	-0.72	0.66	0.73				Whether I wash hands after going to the toilet
			0.61	-0.89			Who I do not like at all
				-0.65	-1.77		My e-mail address
		0.55		-0.76			My grades in school report

Cells with significant Fisher-test only (p<0.05), Cohen's d from odds ratios (larger effect size = darker color)

Pre-service teachers chose item more often than 5th graders (overestimation)

Pre-service teachers chose item less often than 5th graders (underestimation)

Figure 4. *Pre-service teachers over-/underestimating 5th-graders (Cohen's d from Odds Ratio & Exact Fisher-Test)*

DISCUSSION

This study aimed to document with whom children are willing to share what information, if there are differences between Grades and to what degree pre-service teachers can predict the responses of Grade 5 children. The ultimate aim was to formulate ideas of how teachers could start with age-appropriate education of data-protection and privacy. Our results indicate that children experience some information and objects as particularly sensitive (e.g., diaries, deviations and hygiene). In contrast, children indicate that gender, name, and country of residence are the least sensitive information.

More specifically, and in line with Nissenbaum's contextual integrity Framework (Nissenbaum, 2010) we found that some information is more willingly shared with some recipients (e.g., parents) than with others (e.g., the class). In addition, we found that Grade 3 and 5 children differ in what kind of data they share with whom. For example, the Grade 5 children share more personal data with their friends and keep more data from the public than the Grade 3 children. These results are in line with outcomes form developmental studies showing that, for younger children the parents are more important as confidantes, whereas for older children the peers become more and more important (Gardner, 2004) and with the results of a self-report study of Lynch and Cicchetti (1997), which also showed peers becoming the most important confidents over time.

Finally, we found that pre-service teachers tend to overestimate the data children would share with the entire world, including strangers. In other words, the children are more careful than the pre-service teachers expected them to be. This carefulness could be used as a starting point to talk with children about the consequences of sharing data on social media and about who collects and shares digital data with whom.

Implications for teaching

Based on the results of this study we have formulated four recommendations for designing lessons about privacy.

a) The results show that the children already perceive data worth protecting in a differentiated way in their everyday environment and are able to distinguish parameters such as "who tells whom" or "what kind of information is told". Specific situations can be discussed together in class and

further differentiated ("via which medium" or "in which context").

b) When introducing the concept of sensitive data to pupils, use their diary, possibly unwanted behaviors (being mean and lying) and personal hygiene (washing hands) as examples. Children will naturally recognize these as particularly sensitive.

c) Avoid adult conceptions of personal data such as illnesses or grades, as children do not regard these as very private.

d) Use all other people/the whole world as a reference for the loss of control over personal data, as most children are not inclined to share their data with everyone. Take into consideration that this works better for 5th graders who indicated more information they would not share with everybody than 3rd graders.

e) Use the subtle differences children show when sharing data with their parents compared to their friends as an example to talk about nuances in sharing data with different entities. This can be used as a scaffold to talk about other users and companies as recipients of personal data because they are similar yet should be treated differently, too.

An important takeaway is the finding that children do not want to share most of their data with *all other people*. The fact that so many of them still do this to some extent - for example via social media and other services - may simply be due to their lack of knowledge about how these services treat their data. This could be a starting point for future experimental studies and be used as a potential narrative to raise awareness about privacy of digital data in primary school children.

Limitations

There are certain limitations to the interpretation of our results because of our data collection method. For each item, children had to indicate with whom they would share it. We cannot be sure that all children were consistently allocating an item to more than one square or if they sometimes forgot to do this. Especially for the Grade 3 children this procedure might have been causing some cognitive overload. In addition, there were items, such as 'my name' that would already have been known by a couple of the recipients. Such factors might have caused some noise in the data, for example, the finding that only 86 of the 94 children indicated that they would share their name with their parents (see Figure 2).

In addition, we used very general items. For example, we asked children if they would share *pictures* of themselves. But this - as many other items - could also be broken down into *good pictures*, *bad pictures*, *embarrassing pictures* and *flattering pictures*. The same could be said for *username*. This item could be a *social media username*, a *gaming service username* or a *learning management system username*. The necessity for collapsing across variants of personal data into one main category should be considered when interpreting the results of this study.

CONCLUSION

The findings of this study contribute to pedagogical content knowledge about privacy protection, a relatively new, yet important aspect of media literacy. We present concrete suggestions for the design of privacy education learning opportunities by demonstrating how children's real-life non-digital privacy experiences can be used as an entry point to the subject. We showed that children have existing nuanced attitudes about whom they share personal data with. We further showed that children seldom report sharing their personal data with the whole world, what could be used as a scaffold to sensitize them for how they behave in the digital world.

REFERENCES

Adhikari, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing*, *31*(2), 96-110. https://doi.org/10.1080/08911762.2017.1412552

Anttila, T., Selander, K., & Oinas, T. (2020). Disconnected lives: Trends in time spent alone in Finland. *Social Indicators Research*, *150*(2), 711-730. https://doi.org/10.1007/s11205-020-02304-z

Babari, P., Hielscher, M., Edelsbrunner, P. A., Conti, M., Honegger, B. D., & Marinus, E. (2023). A literature review of children's and youth's conceptions of the internet. *International Journal of Child-Computer Interaction, 37*(100595), 100595. https://doi.org/10.1016/j.ijcci.2023.100595

Bakó, R. K. (2016). Digital transition: Children in a multimodal world. Acta Universitatis Sapientiae, *Social Analysis, 6*(1), 145-154.

Baumert, J., & Kunter, M. (2013). The effect of content knowledge and pedagogical content knowledge on instructional quality and student achievement. In *Cognitive Activation in the Mathematics Classroom*

and Professional Competence of Teachers (pp. 175-205). Springer US.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday.* https://doi.org/10.5210/fm.v11i9.1394

Bigelow, B. J. (1977). Children's friendship expectations: A cognitive-developmental study. *Child Development*, *48*(1), 246. https://doi.org/10.2307/1128905

Bronfenbrenner, U. (1979). *The ecology of human development: Experiments by nature and design.* Harvard University Press.

Byrne, J., Kardefelt Winther, D., Livingstone, S., & Stoilova, M. (2016). *Global Kids Online Research Synthesis, 2015-2016.*

Chaudron, S., Di Gioia, R. & Gemo, M. (2017). *Young Children (0-8) and Digital Technology - A qualitative study across Europe. (2018).* European Commission, Joint Research Centre. https://data.europa.eu/doi/10.2760/294383

Chinn, S. (2000), A simple method for converting an odds ratio to effect size for use in meta-analysis. *Statistics in Medicine, 19*(2), 3127-3131.

D-EDK (2016). *Lehrplan 21. Medien und Informatik.*

Corsano, P., Majorano, M., & Champretavy, L. (2006). Psychological well-being in adolescence: The contribution of interpersonal relations and experience of being alone. *Adolescence*, *41*(162), 341-353.

Diethelm, I., Hubwieser, P., & Klaus, R. (2012). Students, teachers and phenomena: Educational reconstruction for computer science education. *Proceedings of the 12th Koli Calling International Conference on Computing Education Research*, 164-173. https://doi.org/10.1145/2401796.2401823

Dong, C., & Mertala, P. (2021). Preservice teachers' beliefs about young children's technology use at home. *Teaching and Teacher Education, 102(*103325), 103325. https://doi.org/10.1016/j.tate.2021.103325

Duit, R. (2007). Science Education Research Internationally: Conceptions, Research Methods, Domains of Research. *Eurasia Journal of Mathematics, Science and Technology Education, 3*(1), 3-15. https://doi.org/10.12973/ejmste/75369

Edelsbrunner, P. A., Schalk, L., Schumacher, R., & Stern, E. (2018). Variable control and conceptual change: A large-scale quantitative study in elementary school. Learning and Individual Differences, 66, 38-53. https://doi.org/10.1016/j.lindif.2018.02.003

Finnegan, S. (2020). How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future. *Seton Hall Law Review, 50*(3), 827-854.

Gardner, H. (2004). *Changing minds: the art and science of changing our own and other people's minds.* Harvard Business School Press.

Hartmann, W., Jurjević, D., Senn, F., Waldvogel, B., & Zuberbühler, U. (2019). *Connected: Medien und Informatik 2: Schülerband.* Lehrmittelverlag Zürich.

Hermida, M. (2019). *EU Kids Online Schweiz. Schweizer Kinder und Jugendliche im Internet: Risiken und Chancen.* Zenodo. https://doi.org/10.5281/ZENODO.2916822

Hermida, M., Imlig-Iten, N., Schrackmann, I., & Marinus, E. (2022). Assessing and priming pre-service teachers' attitudes about online privacy and their protection strategies for social networks, email and cloud storage. *Teaching Education*, 1-18. https://doi.org/10.1080/10476210.2022.2106963

Hichang, C. (2010). Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. *Journal of Information Privacy and Security, 6*(1), 3-27. https://doi.org/10.1080/15536548.2010.10855879

Hill, H. C., Rowan, B., & Ball, D. L. (2005). Effects of teachers' mathematical knowledge for teaching on student achievement. *American Educational Research Journal*, *42*(2), 371-406. https://doi.org/10.3102/00028312042002371

Hipson, W. E., Coplan, R. J., Dufour, M., Wood, K. R., & Bowker, J. C. (2021). Time alone well spent? A person-centered analysis of adolescents' solitary activities. *Social Development (Oxford, England)*, *30*(4), 1114-1130. https://doi.org/10.1111/sode.12518

Kahn, P. H., & Turiel, E. (1988). Children's Conceptions of Trust in the Context of Social Expectations. *Merrill-Palmer Quarterly*, *34*(4), 403-419.

Kattmann, U., Duit, R., Gropengießer, H., & Komorek, M. (1997). Das Modell der Didaktischen Rekonstruktion - Ein Rahmen für naturwissenschaftsdidaktische Forschung und Entwicklung. *Zeitschrift Für Didaktik Der Naturwissenschaften, 3(*3), 3-18.

Kodama, C., St. Jean, B., Subramaniam, M., & Taylor, N. G. (2017). There's a creepy guy on the other end at Google!: engaging middle school students in a drawing activity to elicit their mental models of Google. *Information Retrieval*, *20*(5), 403-432. https://doi.org/10.1007/s10791-017-9306-x

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

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. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), 1-21. https://doi.org/10.1145/3134699

Larson, R., & Richards, M. H. (1991). Daily companionship in late childhood and early adolescence: changing developmental contexts. *Child Development*, *62*(2), 284-300. https://doi.org/10.1111/j.1467-8624.1991.tb01531.x

Larson, R. W. (1990). The solitary side of life: An examination of the time people spend alone from childhood to old age. *Developmental Review: DR*, *10*(2), 155-183. https://doi.org/10.1016/0273-2297(90)90008-r

Liberman, Z., & Shaw, A. (2018). Secret to friendship: Children make inferences about friendship based on secret sharing. *Developmental Psychology*, *54*(11), 2139-2151. https://doi.org/10.1037/dev0000603

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

Lukacs, A. (2016). What is Privacy? The History and Definition of Privacy. In K. Gábor (Ed.), *Tavaszi Szél-Spring Wind 2016. Tanulmánykötet. IV. kötet. Pszichológia- és neveléstudomány, Sporttudomány, Szociológia- és multidiszciplináris társadalomtudomány, Történelem- és politikatudomány* (pp. 256-265).

Lynch, M., & Cicchetti, D. (1997). Children's relationships with adults and peers: An examination of elementary and junior high school students. *Journal of School Psychology*, *35*(1), 81-99. https://doi.org/10.1016/s0022-4405(96)00031-3

Meier, R., Hermida, M., Schrackmann, I., Imlig-Iten, N., & Marinus, E. (2022). Welche schützenswerten Daten teilen Fünftklässler mit wem? Fremdeinschätzung angehender Lehrpersonen, Selbsteinschätzung von Schülerinnen und Schülern und fachdidaktische Konsequenzen. *Atti Del 5° Convegno Sulle Didattiche Disciplinari*, 423-430. https://doi.org/10.33683/dida.22.05.72

Mehta, C. R., & Patel, N. R. (1983). A Network Algorithm for Performing Fisher's Exact Test in r × c Contingency Tables. *Journal of the American Statistical Association*, *78*(382), 427. https://doi.org/10.2307/2288652

Mertala, P. (2020). Misunderstanding child-centeredness: The case of "child 2.0" and media education. *The Journal of Media Literacy Education*, *12*(1), 26-41. https://doi.org/10.23860/jmle-2020-12-1-3

Nebel, M. (2020). Privatsphäre und Privatheit. In *DuD-Fachbeiträge* (pp. 39-51). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-31786-7_4

Nikken, P., Opree, S.J. (2018). Guiding Young Children's Digital Media Use: SES-Differences in Mediation Concerns and Competence. *J Child Fam Stud* 27, 1844-1857. https://doi.org/10.1007/s10826-018-1018-3

Nissenbaum, H. (2010). *Privacy in context. Technology, Policy, and the Integrity of Social Life.* Stanford Law Books.

Papastergiou, M. (2005). Students' mental models of the internet and their didactical exploitation in informatics education. *Education and Information Technologies*, *10*(4), 341-360. https://doi.org/10.1007/s10639-005-3431-7

Pew Research Center. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center, Washington.

Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu*. Publications Office of the European Union, Luxembourg. https://data.europa.eu/doi/10.2760/159770

Sánchez-Meca, J., Marín-Martínez, F., & Chacón-Moscoso, S. (2003). Effect-size indices for dichotomized outcomes in meta-analysis. *Psychological methods*, *8*(4), 448. https://doi.org/10.1037/1082-989X.8.4.448

Schneider, M., & Hardy, I. (2013). Profiles of inconsistent knowledge in children's pathways of conceptual change. *Developmental Psychology*,

49(9), 1639-1649.
https://doi.org/10.1037/a0030976

Schunk, D. H. (1995). Self-Efficacy and Education and Instruction. In *Self-Efficacy, Adaptation, and Adjustment* (pp. 281-303). Springer US.

Shulman, L. S. (1986). Those who understand: Knowledge growth in teaching. *Educational Researcher (Washington, D.C.: 1972), 15*(2), 4. https://doi.org/10.2307/1175860

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU KIDS ONLINE 2020*. London School of Economics and Political Science (LSE).
https://doi.org/10.21953/LSE.47FDEQJ01OFO

Stoilova, M., Bulger, M., & Livingstone, S. (2024). Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use. *Journal of Children and Media*, *18*(1), 29-49.
https://doi.org/10.1080/17482798.2023.2265512

Symantec. (2015). *State of Privacy Report 2015*. https://www.nortonlifelock.com/content/dam/norto nlifelock/pdfs/reports/state-of-privacy-report-en-2015.pdf

Thomas, V., & Azmitia, M. (2019). Motivation matters: Development and validation of the Motivation for Solitude Scale – Short Form (MSS-SF). *Journal of Adolescence*, *70*(1), 33-42.
https://doi.org/10.1016/j.adolescence.2018.11.004

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193. https://doi.org/10.2307/1321160

Wolfe, M. (1978). Childhood and privacy. In *Children and the Environment* (pp. 175-222). Springer US.

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*.

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.*