



universität
wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Titel of the Master's Thesis

“Children, Online Privacy and Data Protection”
Insights from Focus Group Discussions with Children Aged 10-14 years in the
United States

verfasst von / submitted by

Lisa Alfonzo

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on
the student record sheet:

UA 066 550

Studienrichtung lt. Studienblatt /
degree programme as it appears
on the student record sheet:

Masterstudium Communication
Science

Betreut von / Supervisor:

Ass.-Prof. Dr. Claudia Wilhelm

Table of Contents

1. Introduction	4
2. Literature Review	4
2.1 Conceptualizing and Defining Digital Privacy	6
2.2 Dimensions of Children's Online Privacy	8
2.3 Governmental Laws & Regulations in the U.S.	10
2.4 Privacy-Related Risk of Harm	12
3. Method	14
3.1 Research Design (Delimitations, Data Collection & Procedure)	14
4. Qualitative Analysis Focus Group Interviews	18
4.1 Children's Knowledge and Familiarity with Digital Privacy and Data Control	18
4.2 Digital Citizenship & Education	21
4.3 Data Tracing, Risks and Dangers	23
4.4 Autonomy and Decision-Making Process	24
4. Limitations and Ethical Considerations	26
5. Discussion and Conclusion	27
6. References	32
7. English Abstract	38
8. German Abstract	39

Introduction

Internet and media usage among children in the United States has significantly changed over the last decades. There is a constant increasing development of new technologies where new social media apps are often targeted toward children. The Internet provides children the opportunity to explore, grow, and learn. However, the time that children and teens spend online has reached record highs, overtaking time spent watching traditional TV (Ofcom, 2017). The COVID-19 pandemic has led to a rise in screen time and the socialization of children shifted to digital platforms. Across the world the increase was noticeable, and many children's recreational screen time has almost doubled during the pandemic (Korhonen, 2021).

The digital future of young children often depends on the actions the parents take in protecting their children's digital privacy (Isk  l & Joamets, 2021). However, parents often share private information about their children before they are even entering this world. Pregnancy announcements, pictures of newborn babies and many more milestones in a child's life are often documented and posted online without the child's consent and taking their safety into consideration. Oftentimes, parents tend to neglect the fact that they do not own their children's data but are solely the safeguards and legal representatives of the child. This role entails that parents always act in the best interest of the child (Isk  l et al., 2021). However, the rules and regulations to protect children's privacy in the digital age are blurry, insufficiently regulated and enforced.

Public policy and research questions arise especially an increasing concern among parents and lawmakers for children that are growing up in this digital age. Given this increased amount of online activity many challenges and questions emerge. Are young

children and teens responsible for protecting their online data and personal information themselves? If children's autonomy is at the center of public policy are there enough channels to empower teens and children to prioritize their online safety and behavior? How do children value, negotiate and understand their privacy online? Does teaching children about the concept of safe digital citizenship mitigate risks and increase digital safety long term? The dimensions of children's autonomy are often disregarded and their understanding and wants about privacy and personal data protection are not taken into consideration during the process of creating and implementing new policies to safeguard their data online. There is a wide misconception that children do not care about their digital privacy and potential threats. However, research by boyd and Hargittati (2010) has shown that a substantial number of young Facebook users are increasingly getting concerned and are aware of the potential privacy threats.

The question of how children's personal data should be managed or regulated in their best interest and what crucial role organizations, parents, and educators are playing is key in supporting the child's right to privacy (Stoilova., Livingstone & Nandagiri, 2019). There are urgent calls for legislative changes for major platforms such as Instagram, Google, Snapchat, and Facebook to reduce the risk of harm including conduct, content, commercial risk, and contact (Hasebrink, Livingstone & Haddon, 2008). Companies such as Facebook seem to neglect ethical frameworks when developing their privacy protection strategies. Profits are often prioritized and the driving force behind creating digital content and websites that children end up visiting and consuming.

There is ongoing discussion among public legislators and private citizens about if platform should have to accept a certain number of regulations of data privacy. The Federal

Trade Commission's (FTC) Children's Online Privacy Protection Rule (FTC 1998 and updates) was implemented to protect children's online privacy. However, a study of online children's apps showed that more than 50% of the apps failed to protect the children's data (Egelman, 2017). Social networking sites (SNS) are particularly problematic because they are widely unregulated and platforms such as Facebook are well-known for violating the right to privacy.

The explosion of new social media apps and sharing platforms has prompted an increase in research on online privacy and children over the last decade. However, quantitative and qualitative studies that focus on the concept of children's autonomy and its influence on safe digital citizenship are still scarce and relatively new. The new generation of children are considered pioneers and trailblazers when navigating online privacy because they are more likely to experiment and exploring new digital devices, services, and contents (Stoilova et al., 2019). Hence, many children encounter risks online before adults are even aware of them and can create strategies to decrease and mitigate harm.

Conceptualizing and Defining Digital Privacy

Conceptualizing and defining digital privacy can be difficult. One of the classic conceptualizations of privacy is by Westin (1967) who defines it as "the claim of individuals, groups, or institutions to determine themselves when, how and to what extent information about them is communicated to others". Margulis (1977) later pointed out that privacy as a "whole or in part represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (p.10) The terminology and definition of what privacy is has gone under considerable modifications over the years. Interest in privacy related issues has only increased with the increased usage

of the Internet and social media platforms. Many citizens and some corporations are still holding on to the idea that maintaining forms of data protection is crucial and should remain at the forefront of public debate.

The author of the book ‘Children: Rights and Childhood’ David Archard, notes that the United Nations Convention on the Rights of the Child, which was first adopted in 1980, mentions two different approaches to children’s rights. On the one hand, it suggests that children have the right to ‘protection’, and on the other hand children’s right to ‘participation’. Protection implies that a child is defenseless and helpless while participation views children as autonomous and active agents. Nissenbaum’s definition of privacy as ‘neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information’ furthers the notion that it is a delicate balance of children having control of their own data and other channels enforcing regulations (Nissenbaum, 2010).

More recent research by Sarikakis (2017) has shown that “privacy is understood almost universally as a matter of controlling one’s own data, including information disclosure even to friends, and is strongly connected to issues about personal autonomy” (p.1). However, at what age do children have the necessary tools and understanding of how and what kind of information they should share publicly on the Internet. While plenty of research has focused on adult’s awareness and control of their data, a child-centered and qualitative approach is necessary to assess and understand the limits of children’s comprehension of what their privacy rights entail in a digital setting. Even fewer studies have focused on children’s understanding of institutional privacy. This research highlights the need to take children’s autonomy into consideration when creating, drafting, and

implementing new public policies by governmental institutions and parents and educators teaching digital literacy.

Dimensions of Children's Privacy Online

Children's digital privacy is especially relevant because of the rapid development of technology and its risks it poses. Institutional privacy is one dimension that is at the center when discussing data control of children and it entails delegating and shifting control to government institutions (Young & Quanhaase, 2013). According to Stoilova et al. (2021) not much attention has been paid to the discussion of institutional privacy in relation to children especially in literature. It usually is only discussed in relation to collecting data and not raising concerns about children's own privacy practices.

Without universal international privacy laws and laws at the U.S. federal and national level there are not enough policies and regulations to avoid malpractice of the data of a child and avoid negative long-term consequences. According to the U.N. the human right to privacy has never been more important and more threatened (U.N. report 2021). Federal laws to protect children's privacy in the U.S. exist but have some significant limitations. There is a valid reason to be concerned as a recent review of American youths online social network profiles has shown that only 61% of you aged 10-18 years old had their privacy setting enabled and more than half did not turn off their GPS location tracking services in the apps (McAfee, 2014).

The surveillance of the data of children poses many important questions about children's rights. Livingstone (2016) points out how "children's digital rights intersect with existing children's rights instruments such as the United Nations Convention on the Rights of the Child (UN CRC, 1989)".

Livingstone (2016) argues that

Children's lives in the digital age raise new questions about the so-called 3P's of the CRC – rights to provision, protection, and participation – in the changing media and communication environment... As children's daily lives become ever more heavily mediated, and as the media themselves simultaneously converge and diversify, researchers along with policy-makers and the public are now debating whether 'the digital age' is enhancing or undermining children's rights, with current controversies centering on children's right to privacy online as offline, to information and freedom of expression, and to protection from sexual and aggressive threats variously mediated and amplified by the internet. (p. 5)

Even though demands for stricter regulations have become more intense in recent years, the interest in how Internet user's data is protected in the U.S. is not new. After the term "right to be forgotten" ("RTbf") was created in Article 17 of its 2012 general Data Protection by the European Commission legislators, private citizens and public legislators in the U.S. demanded stricter laws. Nonetheless, "RTbf" was considered controversial, and critics referred to it as "rewriting history" and "censorship" (Ambrose, 2013). Although federal laws are required to make significant changes to privacy policies, many U.S. citizens oppose tighter regulations because they are afraid it violates their first amendment right. Nevertheless, even the American Library Association, that defends free speech, acknowledges that privacy upholds the First Amendment of the U.S. constitution. It stresses that it "is absolutely essential to the exercise of free speech, free thought, and free association" (ALA *Manual*, 2002).

Therefore, empowering children to have knowledge and take control over their digital footprint will only encourage them to express themselves safely and freely online in the future. However, the task to find a balance between children's protection and independence is challenging and requires a delicate approach that involves teaching children to effectively protect themselves online (Wisniewski, 2018).

Governmental Laws and Regulations in the U.S.

Governmental institutions are often at the center of national debate regarding children's online privacy. In the U.S. it entails government at all levels such as local, national, regional including states and provinces. However, online privacy is more difficult to govern which makes individuals more vulnerable to online threats. The digital trail of children can be exploited, and their data can be misused. Digital-by-default is increasingly the policy of national governments (Stoilova et al., 2020).

Even though data privacy laws dictate the collection, disclosure and use of personal data companies still violate and mislead consumers about their privacy practices and data security. The Federal Trade Commission (FTC) has taken several actions against companies that decided to not adhere to the rules. In 2012 Google had to pay a \$22.5 million dollar fine reached during a settlement due to misrepresenting its privacy policies to the users of its service. The FTC also held Facebook accountable by fining and making the company pay \$5 billion for deceiving its users and not giving them full control of visibility of their personal information. Facebook was forced to make some significant changes to its privacy measures and disclosures. While the FTC tries to crack down and force companies to adhere and follow regulations the increasing digitalization and people's online habits require strong laws to protect data from exploitation.

COPPA

Undoubtedly, the most significant public law in the United States to uphold children's digital privacy was the Children's Online Privacy Protection Act, also known as COPPA, passed in 1998. Websites and services in and out of the U.S. that are aimed at children aged 13 years and younger must receive parental consent before collecting children's personal

information. The law includes information about how websites can verify consent from guardians and parents and in what ways sites are supposed to protect children's privacy and safety online (FTC regulation). Since the implementation of COPPA there have been numerous privacy conferences and workshops at the FTC focusing on general privacy issues (FTC 2016, Putting Privacy Disclosures to the Test).

While these type of workshops and conferences provide plenty of information about privacy principles there has been limited research on how children respond to receiving education about privacy disclosures and digital privacy rights. Lawmakers, parents, and children acknowledge that COPPA is outdated, and a review and update is necessary to ensure stricter data protection of children. In addition, such legislation cannot protect children from hacking events and data breaches nor from friends, adults, or parents decisions to share details about them online (Williamson, 2017)

A pioneer in legislation and a state that tries to tackle the issue of children's online privacy is California. The recently passed new legislation called California Consumer Privacy Act (CCPA) imposes new restrictions on Internet companies that target minors. It requires companies to keep children's health in mind and it prohibits 8 common data-collection practices. The new California law defines children as all minors up to 18 years old and includes any service that is "likely to be accessed" by children (Slefo, 2019). This new law not only applies to social media apps but also online retailers, news sites, navigations app, education technology platforms, and mobile games. It clearly states that businesses can only sell personal information of a child if they have affirmative authorization ("opt-in") for the distribution and sale of the child's personal information. Even stricter regulations apply to children under the age of 13 where the child's parent or guardian must give consent.

However, since the regulation only applies to California confusion exists about what to do when someone from California visits a different state. Implementing nationwide laws is necessary to force organizational changes inside companies to comply with protecting children's data. Ultimately, companies will have to adapt quickly to any regulation changes that arise as more states pass stricter privacy laws.

Privacy-Related Risk of Harm

Concerns for privacy have only intensified with the advancement of digital technologies and due to the fact that the Internet compiles large amounts of datasets that contain personal information (Selwyn & Pangrazio, 2018). There is a significant amount of literature discussing privacy online risks that children face and at the center of it are online marketing, willingness and awareness to provide personal information online, the effects of privacy disclosures (blackmailing, identity theft, defamation of character), and unawareness of the privacy online policies of digital platforms (Stoilova et al., 2019). Children are particularly vulnerable and more at-risk than adults to privacy online threats because many do not possess the skills yet to use the Internet safely exposing them to privacy risks.

Children's own online behavior have been under scrutiny for privacy risks (Stoilova et al., 2019). Previous research has examined what information children make publicly available online and studies have shown that private information such as list of friends, current city, birth year, graduation year, relationship information, favorite movies, music, and many more are easily accessible by complete strangers (Dey, Ding & Ross, 2013). One study by Steeves and Webster (2008) suggests that children's trust in their social networks makes children less likely to engage in protective behavior and more likely to disclose and share personal information. In their study they surveyed Canadian children aged 11 to 17 and

showed that almost half of them considered it safe to share secrets via online messages and email (45%). This type of risky behavior increased with age making 17 years old the most vulnerable and the most willing to disclose personal information.

A substantial amount of focus has been paid to privacy online risk. However, research and studies about the experience of harm from the risk has been given less attention. According to Stoilova et al. (2019) some studies on the negative effects from privacy risks on young adults do exist, there is a need for more research to investigate and find any potential correlation between privacy risks and harms and their effects on children. Especially teenagers only take measures when the risk has increased and escalated to a potential harmful situation.

In 2013 the DIGCOMP report lists 5 areas of digital competencies which include collaboration and communication, digital content creation, safety, data and information literacy, and problem solving. These areas of competencies are crucial for children to acquire to become responsible digital citizens. However, a study conducted by Martinez-de-Morentin et al. (2021) revealed that girls engage in more risky behavior online than boys. In addition, only 68% of kids think that they can correctly assess if a digital source is reliable or not. This makes children a particular vulnerable group for disclosing sensitive data and their location to strangers that could potentially harm them.

Transgressive or experimental acts often leave a trace that cannot be ignored. In the past, regulators and parents did not pay much attention to teenage digital sexual practices and it stayed mostly out of public debates. However, increasing Internet usage among youth has attracted huge debate over the tension between participation and protection rights (Livingstone, Third, 2017). The online expression of adolescent's sexuality can result in

negative experiences and consequences because it can be shared without permission by recipients exposing users to sextortion, online bullying, and revenge porn. A recent study in the United States has shown that out of 5,593 middle and high school students, 13% of participants reported having engaged in sexting, and 18.5% reported having received one (Patchin & Hinduja, 2019). Further studies have shown that adolescents are particularly vulnerable to engage in sexting due to peer pressure and emotional impulsiveness (Klettke et al., 2014).

Method

Studying the complexity and different dimensions of children's online privacy requires a multi-lateral approach. In the previous section a content analysis of existing literature was used to identify relevant existing research, studies and provide an overview of relevant information. Hence, analyzing and identifying present significant findings on how children navigate the issue of privacy digitally creates a path for further research and recommendations for safer Internet use.

The other method to further explore what role children's autonomy plays in taking ownership of their own digital privacy is to further examine it by conducting focus group interviews among children. Moreover, in focus group discussions, children are given the opportunity to explain, comment and share their attitudes and experiences. In focus group discussions children can engage in a group conversation where the discussion can be guided, monitored, and recorded for research purposes.

Research Design

A total of 6 American children who live in the U.S. between the ages of 10-14 were recruited to guarantee having participants who already have some experience with Internet

usage and digital privacy. Research on children's information processing was considered while choosing the target age group for the focus group interview. Early adolescence (age 8–13) is often a time where children act out and are rebellious (Pickhardt, 2009). Hence, they often go against restraints and neglect to follow safety rules while using the Internet. Such rebellion can lead to high-risk and self-destructive behavior and potentially exacerbate negative consequences.

It is also important to keep in mind that every child is unique, and every child develops at a different pace. The skills children master, acquire, and test at different ages subsequently influence their online negotiations and behavior. Particular attention needs to be paid to the abilities, knowledge, vulnerabilities, and skills of younger users because their decision-making process is still underdeveloped. Children often learn through observing parents, adults or older siblings and interact or decide through trial and error. A study by Livingstone et al. (2016) found that young children (9-11) displayed less competence in managing their online privacy settings than teens (aged 12-17). The desire for privacy increases with age and the understanding of what privacy entails becomes more complex (Chaudron et al., 2018). Children's increasing social media use at a young age and limited knowledge about online safety often results in acting less restricted digitally making them more prone to sharing private information online and vulnerable to stalkers.

I gathered data from children who regularly use the Internet about their awareness of digital laws, policies, autonomy and their privacy practices, and rights. Due to limited access to American children in Austria the interviews were conducted online via Google Meet. Google Meet was chosen to ensure a safe and secure virtual meeting platform. While they are not new, online focus group interviews were conducted because it is a useful modification of

traditional methods. According to Kamberelis and Dimitriadis (2005) “it is applied within the online environment, using conference calling, chat rooms or other online means. Google Meet is more secure than Zoom because it encrypts messages “in transit” which means that they are encrypted between Google’s server and the device. To ensure and guarantee safety of the participants personal information of the Google Meet meeting was only accessible to all participants via an access code. Even though virtual focus group interviews are vulnerable to technical issues such failure to capture non-verbal data and poor or loss of connectivity (Dubrovsky, Kiesler, & Sethna, 1991), Adler et al. (2019) emphasize that focus groups with children have the ability to capture their original ideas, insights, and perspectives, which are often not considered in more traditional child research.

At the beginning of the focus groups a short survey was conducted where the legal guardian and child gave their consent for participation and answered some basic questions. Younger children were not able to consent so the concept of “assent” will be used. Cocks (2006) defines “assent” as a verbal or nonverbal confirmation that participants have grasped “the relationship between the researched and the researcher,...trust within that relationship and acceptance of the researcher’s presence”. Then, the interview guide with different themes helped keep the discussion relevant and on track. The participating children were asked questions about what digital privacy means, what knowledge they have about legal laws that protect their data online, their online privacy practices and experiences, and who they think should control and decide over their personal data. I designed the discussions with a participatory focus and used visuals, workshop activities, real-life scenarios, and games to allow children to engage and have conversations emerge and flow spontaneously. Furthermore, in the short survey I also asked how much time they spend online and

familiarity with relevant digital terminologies such as digital footprint, privacy setting, and user agreement.

In addition, prior to the focus groups interviews children filled out a short survey on demographic data including familiarity with digital apps and Internet usage. In addition, an interview guide was created to guide the discussion and explore different themes. At the core the meaning of personal digital autonomy, control over personal data, institutional responsibilities, and understanding of safe digital citizenship were discussed. The 6 children were split up into two groups of 3 each to make transcription more feasible, increase discussion among children, and not to overwhelm participants. Recruitment took place on social media sites because it allowed to reach out to many U.S. families. After successfully recruiting enough participants, an email confirming the time, date and the invitation link for the online platform were send out. A day prior the interviews a reminder for participants was send out to please fill out the survey. During the interviews the discussion was video, and audio recorded, conducted in English and transcribed word-for-word. An assistant note-taker helped taking notes of observable non-verbal cues and behavior.

I ran two focus group discussions of male and female U.S. based children who are attending school in person (not homeschooled). Participants mean age was 12 (SD=1.41, range 10-14). On average the focus group lasted around 55 min. When further discussion and new information seemed unlikely, the moderator moved the conversation along by introducing a new topic or question. Out of 6 participants, 66% reported that they have and use Internet on their phones or tablets, compared to 34% who did not. On average the kids spend 90 -120 minutes a day online. Instagram is the networking site that most children were familiar with (see Figure 1).

After both sessions a thematic analysis was conducted using LiGRE, an automatic transcription module that facilitates the transcription of audio and video data. The analysis of the focus-group data was performed to extract the most important themes, unexpected findings, and noteworthy quotes (Breen, 2007). The social interactions among the children were put into an analytical perspective to find layers of meaning in the discussion. According to Breen (2007) in “extracting themes from the interviews it is important to take account of the extensiveness, intensity and specificity of comments made, and more weight should be assigned to such quotes.”

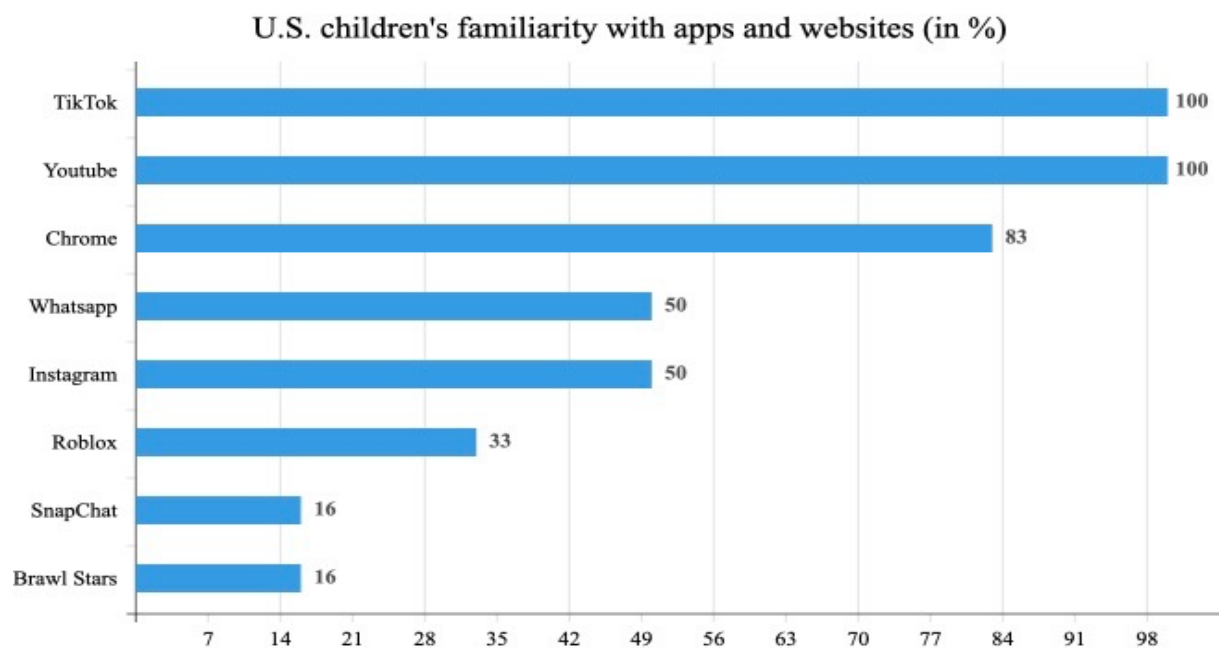


Figure I. U.S. children’s familiarity with online apps and websites (in %).

Children’s Knowledge and Familiarity with Digital Privacy and Data Control

During the discussion, it was evident that the conversation mostly revolved around interpersonal aspects of digital privacy. When participants were asked what privacy means to them the conversation and discussion focused on having control of who can look at personal photos and find out information. Furthermore, when asked how much they think

they are in control over their personal data online, participants agreed universally that they feel they have little control and accepted the lack of control. A common theme was the idea that privacy not only exists virtually but also in real life and the capacity to have control over information. Stoilova et al. (2021) have confirmed that interpersonal aspects are easier for children to comprehend and focus on and give them a greater sense of control and agency.

Children described how they negotiate and decide what information they share when registering for platforms, posting pictures online, and sharing links with others. High importance was placed on protecting their relationships, their privacy but also how it makes them “look” online to express themselves. Children’s concern with what to share and post online and with whom shows that individual control is vital to them and carefully considered. They mostly considered the online environment as a private space for socializing with friends and peers and exercise self-expression.

Many participants showed keen awareness of the risks encountered to privacy while online and a great deal of awareness of reputational damage.

I don’t want to put up something on my feed that makes me look bad or uncool. All my friends see this stuff and I don’t want to offend other people (...) my friends sometimes post some offensive photos, but I just want to stay away from trouble (Boy, 11)

There is some things I don’t want people to know or see about me so I don’t post about it and keep it private [. . .]. (Girl, 12)

Online is my personal space where I decide for myself what I want people to see and who can have access to my stuff and info. I love to paint and post my art online. I get new ideas from other artists and I love to share and express myself through art (Boy, 14)

I love to do makeup and upload videos on YouTube. At the beginning, I made all my videos private and only shared them with my closest friends. Now, I’m more confident and my videos are public. Sometimes, I get hateful

comments and I think about changing my account back to private but I love to that other makeup artists can see my videos and give me advice and tips (Girl, 13)

While some children were able to differentiate between different privacy settings on SNS (public versus private profile), all the participants were less familiar with institutional privacy which entails the collection of meaningful data such as medical records, school, or government. Children did not consider school records, immunizations, attendance in school or academic grades as personal data. These types of data collection are considered ‘ordinary’ and ‘common’, so participants usually do not give them much consideration. According to Stoilova et al. (2021) children ‘expect to be monitored both digitally and offline to ensure their compliance with an established code of behavior’. These results support Stoilova et al. (2019) findings that children are more likely to focus on the data that they voluntarily share than the data that is collected from them because they feel it does not affect them. Children’s trust in public institutions is an ambivalent phenomenon because it serves as a social function and often provides basic needs.

I don’t care if my school keeps and collects my information like my date of birth, social security number, and grades. That’s just standard procedure and that’s how it works nowadays. Everything is online. (Girl, 13.)

It’s my school so I trust it to keep my information safe (Boy, 11.)

I trust my doctor. He just needs my records for helping me when I’m sick. (Girl, 10)

Institutions collecting children’s data was not a cause for concern and considered justified to ensure their safety and their well-being. Hence, doctors keeping medical records

was viewed as standard procedure and necessary to treat patients and make an effective diagnosis. In addition, many respondents

Digital Citizenship and Education

Today's children can be seen as active citizens with meaningful and complex opinions. Their ability to play and learn gives them a meaningful contribution to their environment. "Citizenship is the social and legal link between individuals and their democratic political community" (Patrick, 2000). On the one hand, children are seen as autonomous individuals, on the other hand, as objects of protection (Jans, 2004). It is absolutely vital to understand that children are emerging digital citizens that must be taught the right tools to successfully contribute and fulfil their responsibilities in a democratic society (Philipps, Ritchie, & Adair, 2020). Data literacy is a complex concept that is generally not grasped or taught to children by their parents or formal educators. It is a learning process that leaves many misconceptions and gaps including policies that are hard to understand for children.

I still don't understand the terms they use. It's confusing language and wordy and I just don't get it, so I usually just click agree (Girl, 12)

If my friends have the app.....I just download it and trust it (Boy, 14)

I usually don't read the privacy policy. I already know Facebook is tracking everything I post on there, but they make it really hard to change the settings. One time I wanted to delete my account and couldn't. I didn't find the page where you can delete it, so I kept it (Girl, 13)

A common theme emerging from the discussions was that children are confused by terminologies used when signing up for an account on an app or other type of website. Children are less inclined to read the fine print on the service or user agreements when signing up for a new account online or downloading a new app. In 2016 researchers from

Carnegie Mellon University compared and examined written privacy policies of almost 18,000 free apps that were created for children to the computer code that ran the applications (Spice, 2016). The results showed that more than 9,000 apps had privacy policies. However, half of them deceived users by not being honest about what information the app really collected. The code revealed that the apps did not adhere to the privacy policies that they users had agreed to by collecting time-on-task data and location without authorization. Furthermore, 17 percent disclosed data with other companies without stating it in their privacy policies. Children often trust big companies to protect their privacy and think they would not break the law because it could ruin their public reputation and make users lose trust. When asked how confident participants feel about making privacy decision online more than half of participants reported not feeling very confident.

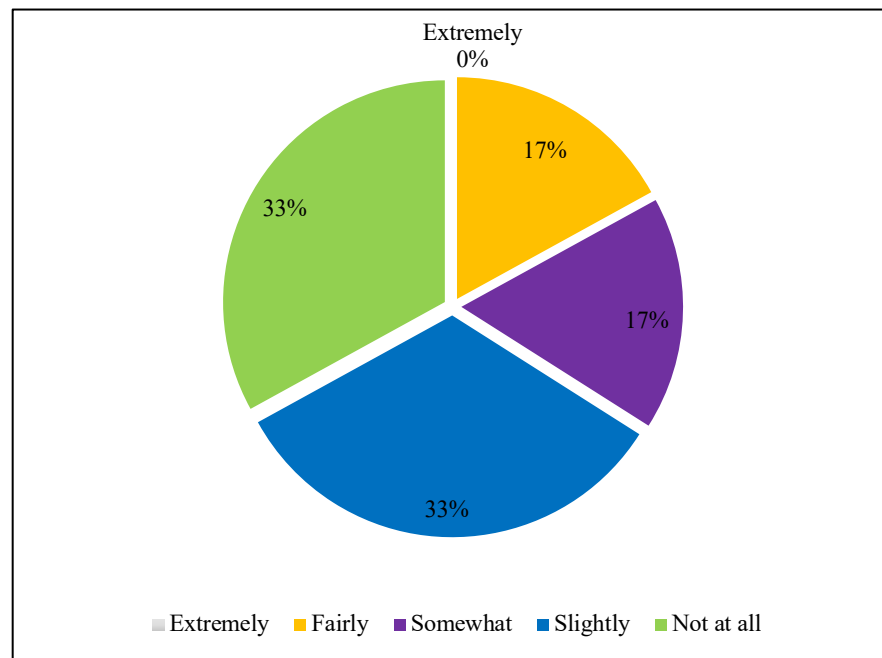


Figure 2. Participants' confidence in making privacy decisions online (in %)

Less than half of the participants reported having some discussions and formal education about digital privacy in school before. Noticeably, all children who had prior

training by an educational institution (school seminars or classes about safe digital citizenship) acknowledged and mentioned that they are aware that they never have full control over their data. Marwick and boyd (2014) describe it as ‘networked privacy’ which refers to the public-by-default nature of online communication. However, these children who had formal education reported feeling more confident about protecting their privacy online and deciding what to share digitally.

Data Tracing, Risks and Dangers

Overall, participants were less worried about data tracing and privacy. Children were only concerned about data tracing when their physical safety could possibly be compromised. Hence, children are more vulnerable than adults and more susceptible to harm. Many participants acknowledged the need for boundaries when sharing personal information online to prevent harm and damages.

I’m worried about like some weirdo following me home if I post an Instagram story when I’m out so I post it later when I get home. (Girl, 13)

I’m careful. There are people out there who try to steal passwords to my account.....you should not accept friend requests from strangers who you’ve never met or talked to. They could turn out to be hackers, bullies or sexual predators (Boy, 14)

I have a friend whose brother was moving away to college. Her mom posted a photo of that brother with the caption ‘off to college’ and then the name of the university; her profile is not private. Everyone will know where he goes to school and can track him down. Not OK. (Boy, 11)

I always make sure that I switch off the tracking feature in the Apps I’m using. I don’t like that Apps try to track my every move and know everywhere I go. (Boy, 12)

Risks of privacy were only considered when it could possibly lead to a harmful situation.

Livingstone (2014) supports this notion by pointing out that children often think about the risks in terms of worst-case scenarios. Previous studies have confirmed that interpersonal risks seem more relevant to children than institutional risks of long-term collection of personal data (Lupton & Williamson, 2017). Children and parents do not always agree with

what classifies as risks online. Parents and children have different motivations and reasons using media and do not always see eye-to-eye when trying to reduce the risk of harm.

Haddon et al. (2017) give some examples of different assessment of opportunities like “meeting a new person online is generally an opportunity as children see it but a risk to their parents; giving out personal information online enables children to pursue new opportunities but worries their parents; looking up sexual information is vital for many teenagers but can seem like an obsession with pornography, and something to be filtered or blocked, to many parents.”

Autonomy and Decision-Making Process

Throughout the interviews it was evident that every child placed importance on having a say in who has access to their data. It is commonly assumed that children do not have the capacity for autonomy or that they are lacking the competency to make rational decisions. According to Giesinger (2019) children do have certain rational capacities from early on and are capable of authentic attitudes. Children take their desires, views, and values into consideration before making a decision. Children are less able than adults to avert being harmed since they are lacking certain agency-related capacities. However, children think that they should control and have the final say in what is being shared digitally. A recent online survey of 331 parent-child pairs (children aged 10-17) in the U.S. showed that there is a disconnect between parents and children on what to share. Parents and children disagree on the permission-seeking process when it comes to sharing and posting information online (Moser et al., 2017)

During the discussion, children felt uneasy about the lack of control and disregard for personal choices when parents share pictures with friends or family members on social media

sites or messaging apps. Half of the participants felt it breaches their right to privacy and takes away from making the decision of what to share. Some participants also mentioned intervention and prevention strategies to avoid “unexpected” posts from their parents, friends or relatives. Children were quite informed about some of the options to preserve their online image. These strategies on SNS included setting their accounts to private, having to give permission when being tagged, and blocking people. Setting the account to private seemed the most important and drastic measure for restricting the spread of posts.

I know my mom shares photos of me in WhatsApp with friends and family. I told her I don't want that because I might not like the way I look in a photo and I don't want her friends to know everything I'm doing.....she listened and stopped doing it. Now, she always asks for my permission before sending pictures to family members.
(Girl,13)

“My parents don't delete them because they think it's cute, then I get really angry and I try get into their account and delete them myself.” (Boy, 13)

On Instagram, I made sure I put my account on private. Only people I know and approve can follow me. You can also make your account public, which means that everyone can follow you but I don't want people I don't know look at my stories and posts. (Girl, 14)

Children were mostly concerned with parents sharing pictures and “embarrassing” stories on social media platforms such Instagram and Facebook. There sometimes is also the concern for unwanted and unnecessary communication among participants.

Some people and friends will put up anything online. They tell me things I don't care about or want to hear.....like the food they eat. They'll take a picture of stuff I couldn't care less about and send it to me (Girl, 10)

[. . .] like photos of me on my mom's Facebook.....I don't like that. I want to decide what I share with my family and friends (Boy, 12.)

'When my friends take pictures, I don't mind it because I trust them, I know many of their followers. I don't have a problem with that. (Girl, 12)

Children were also worried about the contradictions between the online persona they are trying to construct, and the photos and posts parents might share potentially leading to embarrassing situations. Participants emphasized that parents should respect boundaries and carefully consider and ask for permission before posting about their children.

Limitations and Ethical Considerations

There were a lot of different ethical considerations conducting research with children. Focus group interviews (FGI) are gaining popularity among scholars in research in particular in children and parent research. It gives all participants the opportunity to share their own story and a voice to express their opinion. In addition, it encourages a conversation among participants that allows for an open and free discussion without a strict order of questions. However, working with children and parents posed its own challenges and the FGI had to be carefully planned. Important factors in particular ethical aspects were considered to safely plan, analyze and conduct FGI with children and parents. Consent is a central ethical concern in research and is at the forefront of human research. In particular, digital privacy might be a sensitive topic where consent is vital. Hence, both parents and children had to give consent to participate in the discussion. Disclosing the potential risks such as challenges that arise while conducting FGI virtually was key in having and providing a safe space for discussion. Furthermore, lack of information and inadequate disclosure upfront would be a constraint upon autonomous decision making (Beauchamp 1997).

The concept of children's agency and voice is another important consideration because children are social beings who negotiate complex social relations (Castro, Swauger & Harger, 2017). This is often ignored or forgotten in research encounters which privileges the individual voice due to an in under-interrogated definition of what agency is (Castro et al., 2017). According to Ingrid et al. (2017) "recognizing the ways in which participatory methods, agency, and voice can and should promote reciprocal and relational social realities is vital to a better understanding of the worlds of children". It helps to illuminate and highlight a better understanding of the social realities of children's lives.

Conducting the interviews online also had some limitations. Experiencing some technical difficulties during the interviews, not being able to pick up nonverbal cues, internet instability, and distractions were some challenges that arose. One of the ways to overcome technical difficulties was to encourage early log on times and having technical support for all participants when they entered the session. Even though participants might have been more comfortable conducting and participating in the interviews online, there are often more distractions at home. Clarifying and giving clear instructions to remove any type of distraction aided participants to focus on the interviews.

Discussion and Conclusion

While research on children's interpersonal privacy exists, less focus is being paid to institutional privacy and the responsibilities institutions have to protect children's data. This leaves a research gap that needs to be further explored and studied to fully comprehend the way children navigate sharing personal data. Evidence suggests that children struggle to manage and understand the dimensions of sharing their personal data online and a more multilateral and comprehensive approach is needed to fill in the gaps. While qualitative

research is beneficial to understanding the mindset and attitudes of children by using a quantitative approach, researchers can identify prevalence rates and gain more insight into a larger group of children.

Whilst this paper provides important insight into the field of children's perceptions of digital privacy and practices, it does have some limitations. Firstly, although focus group discussions are valuable, small discussions do not provide the same insight as conducting larger group discussions. Larger discussions are more feasible in an in-person environment versus online. Although the discussions showed children have clear views and are not afraid to voice their opinion on digital privacy, a qualitative survey with a large sample provides broader viewpoints and trends can be more easily identified. A longitudinal field survey could measure changing opinions and practices of how children manage their online privacy as they age and get older. Lastly, this study was conducted in the United States and attitudes and opinions about privacy can vary greatly across different cultures. In the U.S. data collection laws are less restrictive and largely under-regulated compared to the European Union. Research is necessary to recognize and find differences among children in different countries. In summary, this is just a starting point for future research and provides some valuable implications.

The findings have also demonstrated and supported the notion that interpersonal aspects of privacy are easier for children to understand. Children have strong convictions and opinions about what and whom they share data online with and want to decide for themselves how to manage their data. Adults must understand and acknowledge that children have a strong sense of autonomy and they have the right to participation when creating guidelines and policies to protect them. Parents controlling their children's data and online behavior

online often backfires as boyd et al. (2004) have shown in their study that if children and parents disagree, children are likely to act out and try to bypass parental restrictions at mediating the Internet.

It is vital for children to understand the digital environment and grow up to have the skills needed to navigate the complexity of online privacy. Fostering and teaching children's digital skills and safe digital citizenship means understanding the scopes of the digital environment and consent. When deciding policies and regulations there is an urgent call to have a more child-focused approach that recognizes children's voices and takes into consideration their autonomy, capacities, and competencies. More work needs to be done to create better policies and industry standards of data collection and control of privacy settings. Mitigating potential privacy-related harm and educating children about the responsibility of safeguarding their data should be at the forefront of any type of research. The results of the focus group discussions add to existing research and lay fruitful groundwork for further studies that aim to investigate the decision-making process of children. It emphasizes the importance to hear children's voices and their wish to exercise agency and autonomy to not face risks in the digital environment.

This research has also shown that children do not give much thought to institutional privacy and how public agencies like health institutions, government, and educational organizations handle and gather their data. Blind trust in institutions and a general acceptance that data control is delegated to external agencies seems to be norm and can be problematic. Questions remain about children's rights, informed consent and how children experience institutional privacy. Further research must consider if children would like to be able to negotiate institutional privacy and if they feel competent to do so.

Children should not be expected to solely manage and handle their online behavior and privacy protection. It is a delicate balance between ensuring children's own agency and governmental, parental, and educator's responsibility to create a safe digital environment for children. This requires a more multidimensional research on children's data and privacy online. Children show awareness of the risks to privacy while online and learning through experimentation and exploration with technology can aid in effectively evaluating risks and navigating the Internet safely.

Digital literacy education and interactive learning programs have shown to improve children's privacy awareness, risk aversion, and build confidence. Results from previous studies (Andrews, Walker, Kees, 2020) also found that children who have a higher motivation to restrict sharing had a more favorable change in their online safety beliefs. Children are curious learners who have impressive learning abilities that adapt quickly to new environments. The Internet is constantly evolving requiring children, educators, parents, and institutions to quickly adapt to the changing online environment. Children must use all the resources available to keep up with new developments, regulations, and policies to acquire and maintain all the necessary skills to safely use and browse the Internet.

Educators can take advantage of children's learning abilities to maximize digital competencies among children and minimize the effects and potential risks of unsafe online behavior. This research has shown that children feel overwhelmed with the complexity of privacy online. Digital literacy programs that explain and teach terminologies, user agreements, website tracking practices, information evaluation, and social media privacy policies are a helpful tool to support children in feeling more confident and independent in making smarter and safer choices about personal information disclosure on the Internet.

While it is a challenging task to balance children's protection and independence, research suggests that good support and encouragement can make a difference. Instead of exercising restrictive parenting and suppressing children's wishes and voices, enabling mediation and listening to children's opinion is empowering and gives children a platform to learn independently under guidance to apply protective behaviors online. Parents, institutions, and educators must accept that the Internet and in particular social media are part of growing up and will play an increasing role in the lives of their children.

References

- Adler, K., Salanterä, S., & Zumstein-Shaha, M. (2019). Focus Group Interviews in Child, Youth, and Parent Research: An Integrative Literature Review. *International Journal of Qualitative Methods*, 18. <https://doi.org/10.1177/1609406919887274>
- Ambrose, M.L., Ausloos, J. (2013). The right to be forgotten across the pond. *Journal of Information Policy*, 3, 1–23. Retrieved from http://www.jstor.org/stable/10.5325/jinfopoli.3.2013.0001#pdf_only_tab_contents
- American Library Association (2002). Privacy: An interpretation of the library bill of Rights, *American Library Association Intellectual Freedom Manual* (7th ed.). Chicago: American library Association [“ALA Manual”].
- Andrews, Walker, K. L., & Kees, J. (2020). Children and Online Privacy Protection: Empowerment from Cognitive Defense Strategies. *Journal of Public Policy & Marketing*, 39(2), 205–219. <https://doi.org/10.1177/0743915619883638>
- Archard, D. (2006). The Moral and Political Status of Children, *The Author Journal Compilation*, London, ippr.
- Beauchamp, T.L. (1997) *Informed consent*. In: Veatch, R.M. *Medical Ethics*, Jones and Bartlett, 185–208
- boyd, & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8), NP–NP. <https://doi.org/10.5210/fm.v15i8.3086>
- Breen, R.L. (2006) A Practical Guide to Focus-Group Research, *Journal of Geography in Higher Education*, 30:3, 463-475, DOI: 10.1080/03098260600927575
- Cocks A. (2006). The ethical maze, finding an inclusive path towards gaining children’s agreement to research participation, *Childhood*, 13, 247–266.

Chaudron, S., Di Gioia, R. and Gemo, M. (2018) Young children (0-8) and digital technology. A qualitative study across Europe. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union, 1-259.

Castro, I., Swauger, M., Harger, B. (2017). *Researching Children and Youth, Methodological Issues, Strategies, and Innovations*: Vol. First edition. Emerald Publishing Limited.

Dey, R., Ding, Y. and Ross, K.W. (2013) Profiling high-school students with Facebook: how online privacy laws can actually increase minors' risk. *Proceedings of the 2013 Conference on Internet Measurement*. Barcelona, Spain.

Dubrovsky, V., Kiesler, S., & Sethna, B. (1991). The equalization phenomena: Status effects in computer-mediated and face-to-face decision-making groups. *Journal of Human-Computer Interaction*, 13, 133–152.]

A. Ferrari, (2013) DIGCOMP: A Framework for Developing and Understanding Digital Competence In Europe. Luxembourg, Germany: Publications Office of the European Union.

Egelman, S. (2017). "We Tested Apps for Children. Half Failed to Protect their Data," *The Washington Post*, Retrieved from: 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.

Giesinger, J. (2019) Vulnerability and Autonomy – Children and Adults, *Ethics and Social Welfare*, 13:3, 216-229, DOI: 10.1080/17496535.2019.1647262

Haddon, L., & Livingstone, S. (2017). Risks, opportunities, and risky opportunities: How children make sense of the online environment. In P. Brooks & F. Blumberg (Eds.), *Cognitive development in digital contexts* (pp. 275–302). San Diego, CA: Elsevier

Iskül, A, & Joamets, K. (2021). Child Right to Privacy and Social Media – Personal Information Oversharing Parents. *Baltic Journal of Law & Politics*, 14(2), 101-122.
<https://doi.org/10.2478/bjlp-2021-0012>

Jans, M (2004). Children as Citizens. *Childhood (Copenhagen, Denmark)*, 11(1), 27–44. <https://doi.org/10.1177/0907568204040182>

Kamberelis, G., & Dimitriadis, G. (2005). Focus groups: Strategic articulations of pedagogy, politics, and inquiry. In N. K. Denzin, & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research*, 3rd ed. (pp. 887–907). Thousand Oaks, CA: Sage Publications Inc.

Klettke, B., Hallford, D. J., & Mellor, D. J. (2014). Sexting prevalence and correlates: A systematic literature review. *Clinical Psychology Review*, 34(1), 44–53.
<https://doi.org/10.1016/j.cpr.2013.10.007>

Korhonen. (2021). The good, the bad and the ugly of children's screen time during the COVID-19 pandemic. *ACTA PAEDIATRICA*, 110(10), 2671–2672.
<https://doi.org/10.1111/apa.16012>

Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications: The European Journal of Communication Research*, 39(3), 283–303.

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–670. <https://doi-org.uaccess.univie.ac.at/10.1177/1461444816686318>

Lupton, D., & Williamson, B. (2017). The datafied child. *New Media & Society*, 19(5), 780–794.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33(3), 5–21.

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051–1067.

McAfee (2014), “Cyberbullying Triples According to New McAfee 2014 Teens and the Screen Study”, *McAfee 2014 Teens and Screen Study*, Retrieved from: <https://mcafee-dr.mcafee.com/us/about/news/2014/q2/20140603-01.aspx>.

Moser, C., Chen, T., Schoenebeck, S.Y. (2017) Parents' and children's preferences about parents sharing about children on social media. *Human Factors in Computing Systems*, 5221-5.

Nissenbaum, H. (2010) Privacy in context. Technology, policy, and the integrity of social life. Stanford: Stanford University Press.

Ofcom (2017), “Children and Parents: Media Use and Attitudes Report”, Retrieved from: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

Patchin, J. W., & Hinduja, S. (2019). The nature and extent of sexting among a national sample of middle and high school students in the U.S. *Archives of Sexual Behavior*, 48(8), 2333–2343. <https://doi.org/10.1016/j.jadohealth.2018.06.031>

Philipps, L. G., Ritchie, J., & Adair, J. K. (2020). Young children's citizenship membership and participation: comparing discourses in early childhood curricula of Australia, New Zealand and the United States. *Compare: A Journal of Comparative and International Education*, 50(4), 592-614.

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>.

Sarikakis K., & Winter, L. (2017). Social Media Users' Legal Consciousness About Privacy. *Social Media + Society*, 3(1), 205630511769532.
<https://doi.org/10.1177/2056305117695325>

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

Slefo, G. (2019). BRACING FOR SWEEPING NEW DATA PRIVACY LAW; How brands are preparing as the California Consumer Privacy Act becomes a reality in 2020. *Advertising Age*, 90(20), 22.

Spice, B. (2016). Mobile App Behavior Often Appears at Odds with Privacy Policies – News – Carnegie Mellon University.
<https://www.cmu.edu/news/stories/archives/2016/36ovember/mobile-app-behavior.html>

Steeves, V. and Webster, C. (2008) Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology and Society* 28(1), 4-19.

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

Stoilova, M., Livingstone, S., Kardefelt-Winther, D. (2016). Global Kids Online: Researching children's rights globally in the digital age. *Global Studies of Childhood*, 6(4), 455–466. <https://doi.org/10.1177/2043610616676035>

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society*, 24(4), 557–575. <https://doi.org/10.1080/1369118X.2019.1657164>

Wisniewski, P., Jia, H., Xu, H., et al. (2015) 'Preventative' vs. 'reactive': How parental mediation influences teens' social media privacy behaviors. *Association for Computing Machinery, Inc.*, 302-16.

Westin, A.F. (1967) Privacy and freedom. New York: Atheneum.

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

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>.

Martinez-de-Morentin, Lareki, A., & Altuna, J. (2021). Risks Associated With Posting Content on the Social Media. *IEEE-RITA*, 16(1), 77–83. <https://doi.org/10.1109/RITA.2021.3052655>

Abstract

Children are spending more time than ever online and the impact it has on their privacy is evident. This generation of American children is digital-by-default and has very little control over their data and privacy online. This article explores the ways American children understand the concept of privacy online and their awareness of privacy policies and regulations. Through focus group interviews this article looks at the ways children understand and negotiate privacy online and what role the understanding of privacy laws plays in negotiating their online behavior. Firstly, the results indicate that interpersonal aspects of privacy are easier for children to comprehend and give them a greater sense of autonomy and agency. Additionally, participants only consider the privacy risks of data tracing in terms of potential physical harm. Secondly, respondents have a lack of awareness of institutional privacy and children put blind faith in institutions to keep their data safe. Lastly, participants confidence in making privacy decisions online increases with digital literacy programs and education. These findings are consistent with previous research showing that children have a strong sense of agency and highlights the importance of implementing and teaching privacy education to increase confidence and support their autonomy to strengthen the digital skills of the next generation.

Keywords: children, online privacy, autonomy, legal consciousness

Zusammenfassung

Kinder verbringen mehr Zeit als je zuvor online und die Auswirkungen auf ihre Privatsphäre sind offensichtlich. Diese Generation amerikanischer Kinder ist von Natur aus digital und hat nur sehr wenig Kontrolle über ihre Daten und Privatsphäre im Internet. In dieser Masterarbeit wurde analysiert wie amerikanische Kinder das Konzept des Datenschutzes im Internet verstehen, wahrnehmen und wie und ob sie sich der Datenschutzrichtlinien und -vorschriften bewusst sind. Mit der Hilfe von Fokusgruppeninterviews wird untersucht wie Kinder den Datenschutz im Internet verstehen und aushandeln und welche Rolle das Verständnis der Datenschutzgesetze bei ihrem Online-Verhalten hat. Die Untersuchung hat gezeigt, dass zwischenmenschliche Aspekte der Privatsphäre für Kinder leichter zu verstehen sind und ihnen ein größeres Gefühl von Autonomie und Entscheidungsfreiheit vermittelt. Darüber hinaus betrachten die Teilnehmer Datenschutzrisiken bei der Datenspeicherung nur im Hinblick auf potenzielle körperliche Schäden. Weiters mangelt es den Befragten an Kenntnis für Privatsphäre von Institutionen, und Kinder vertrauen blind darauf, dass Institutionen ihre Daten schützen. Schließlich steigt das Selbstvertrauen der Teilnehmer, Entscheidungen zum Datenschutz online zu treffen, durch Programme zur digitalen Kompetenz und Bildung. Diese Ergebnisse stehen im Einklang mit früheren Forschungsergebnissen, die zeigen, dass Kinder ein starkes Gefühl der Handlungsfähigkeit haben. Sie unterstreichen die Notwendigkeit, dass Datenschutzerziehung vermittelt werden muss um das digitale Selbstvertrauen von Kindern zu stärken.

Schlagerwörter: Kinder, Online Datenschutz, Autonomität, Rechtsbewusstsein