Forum Privacy and Self-Determined Life
in the Digital World

PRIVACY AND CHILDREN'S RIGHTS

White Paper

Imprint

White Paper
PRIVACY AND CHILDREN'S RIGHTS

Authors

Ingrid Stapf[1], Judith Meinert[2], Jessica Heesen[1], Nicole Krämer[2], Regina Ammicht Quinn[1], Felix Bieker[3], Michael Friedewald[4], Christian Geminn[5], Nicholas Martin[4], Maxi Nebel[5], Carsten Ochs[6], Lea Watzinger[1], Andreas Baur[1]

Affiliation

(1) University of Tübingen, International Center for Ethics in the Sciences and Humanities (IZEW)
(2) University of Duisburg-Essen, Department of Social Psychology - Media and Communication
(3) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
(4) Fraunhofer Institute for Systems und Innovation Research ISI, Karlsruhe
(5) University of Kassel, Project group: Constitutionally Compatible Technology Design (provet) at Research Center for Information System Design (ITeG)
(6) University of Kassel, Department of Sociological Theory

Editors

Michael Friedewald, Alexander Roßnagel, Christian Geminn, Murat Karaboga

Translation and language editing

Oduma Adelio, Danielle Schmitz

Series

Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

ISSN-Print	2199-8906
ISSN-Internet	2199-8914
DOI	https://doi.org/10.24406/publica-793

Edition

February 2023, 2nd edition
Fraunhofer Institute for Systems und Innovation Research ISI, Karlsruhe

Citation recommendation

Stapf et al. (2023): Privacy and Children's Rights. Eds. Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, White Paper, Karlsruhe: Fraunhofer ISI.

Content

1 Introduction

With the rise of surveillance-based media technologies – such as smart toys, nanny cams, voice assistants such as Alexa, technology enhanced personalized learning, tracking apps, and daycare video surveillance – urgent questions of children's right to privacy emerge. What do we mean when we speak of privacy for children[1]? Are different concepts needed for children's rights to privacy compared to those of adults? To whom should children be able to claim their privacy rights? How do they gain control over the protection of their data as they grow older? Additionally, who bears the responsibility of ensuring this protection?

At both the European and international level, frameworks and legal conditions for the protection of children's and young people's digital rights vary widely. Furthermore, there are countries that are only just beginning to develop a state anchoring of children's rights in the digital space (Sofian et al., 2021).

This white paper analyzes children's right to privacy by drawing on digital environment perspectives from media psychology, media ethics as well data protection law. It refers to current empirical data and formulates demands for policies, media regulation, the education sector, and media providers (see Stapf et al., 2021a). It analyzes German and international regulations and legal debates. *We argue for a stronger enforcement and consideration of children's rights in the digital world since society has a particular responsibility toward protecting children. Among these are the rights to informational self-determination and data protection, the free development of personality, and the right to privacy (Art. 7 CFR)*. The aim of this white paper is to initiate a socio-political discourse, formulate and implement preliminary requirements for practical application, and highlight the need for research – especially in the field of media literacy and education – to develop adequate concepts for specific target groups.

Civil rights of freedom and equality should allow children the right to an open future. Given that childhood is a particularly vulnerable phase of development and important abilities are still being formed, children need comprehensive protection by those who provide care as well as the authorities. At the same time, however, children should be able to have self-determination as active subjects. For this purpose, empowerment measures, which aim at ensuring the autonomy of children in democratic and digital societies, are essential. The issue of children's privacy is ambivalent: on the one hand, it can be understood as a protection measure in the interest of the child, on the other hand, it can include paternalistic surveillance practices that undermine children's claims to self-determination.

The use of digital media is becoming increasingly common in children's lives and requires action with respect to the associated risks. Children and adolescents up to the age of 18 account for about one third of all internet users worldwide. With a nuanced academic examination of the interplay between privacy and children's rights, this white paper aims to fill an outstanding gap (Stapf et al., 2021b).

Children's rights were established under international law in the UN Convention on the Rights of the Child (UNCRC) in 1989 – as a supplement to universal human rights – and have been considered ordinary law in Germany since 1992. Children's rights are also guaranteed in Article 24 of the EU Charter of Fundamental Rights (CFR). The UNCRC emphasizes the role of children as independent

[1] This paper follows the definition of the United Nations Convention on the Rights of the Child which states that "[…] a child means every human being below the age of eighteen years […]".

actors with their own rights and establishes in 54 articles "the best interests of children" as the guiding principle in the interplay of protection, promotion, and participation rights. Furthermore, Article 16 of the UNCRC articulates the right to "protection of privacy and honor."

In 2021, the UNCRC General Comment No. 25[2] was published, which for the first time elaborates on children's rights in the digital sphere. A significant part of the comment deals with privacy (11–12). Numerous stakeholders were involved in a complex commenting process during the development of this document. It was later translated into child-friendly language by children.

Current developments regarding the inclusion of children's rights into the German constitution require a discussion about the significance of the problems surrounding children's right to privacy in the digital sphere. This paper initiates this debate and contributes to reinforcing the protection of children's digital rights, within the contexts of both German and international law (Lorenz & Schomberg, 2022).

[2] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

2 Privacy in the context of digitalization

The relevance of privacy protections in the digital space is rapidly increasing. Childhood is not only a biological phase of life, but it is also socially and culturally constructed. A highly protective view of children often dominates Western social and cultural perspectives. This is based on the idea that children need protected spaces to test and develop their personalities and autonomy. A child's room, for instance, has long been considered a space of retreat, where children's desires for their own private space can be met as well as where personal experiences and relationships can develop (Brown & White, 2014).

While digitalization offers broad access to media content, global platforms, and a wide range of information, it also discloses a lot of children's personal data. One day that this happens is in the context of active, self-initiated disclosure. For instance, when a social media profile contains personal information and photos. Likewise, active disclosure happens when data and information are exchanged through interactions with other users. Additionally, so-called passive disclosure, through the collection, analysis, and sale of data by companies, is also a risk that children are not fully aware of (vertical privacy threat). Children are also increasingly exposed to cyberbullying attacks (horizontal privacy threat). Another option is described as a trade-off in which children must negotiate where their priorities lie: either having a sense of social belonging by being connected through online platforms or making sure their data is protected. The immediate effect felt by staying connected online often takes priority and tends to outweigh the obscure and temporally distant downside of making personal data and information public (Santer et al., 2021).

The notion of privacy in digital contexts

Privacy is an essential condition for democracy and the rule of law, as it functions as the foundation for self-determination and freedom of choice. The concept of privacy is not an independent legal category, but rather encompasses numerous subsidiary aspects. These include various fundamental rights, such as the right to informational self-determination, the right to respect for private and family life, and the right to data protection. Likewise, it comprises other aspects like personality rights, secrecy of correspondence, the inviolability of the home, and the so-called IT fundamental right[3], which aims to ensure the confidentiality and integrity of information technology systems.

In the digital domain, the right to informational self-determination is central. It is structurally very different from the paternalistic approach where the area deemed worthy of protection is determined from the outside through social norms. Instead, the *individual's* self-determination is the standard (Geminn & Roßnagel, 2015; Nebel, 2015). In a protectionist approach, third parties, namely state authorities, the judiciary, and legal scholars, determine what is "private" and thus, protected. This externally determined notion is imposed on the individual. The starting point of the approach is, therefore, the state which defines the boundaries of "privacy". In contrast, informational self-determination is based on a freedom-oriented approach that emphasizes the autonomous decision-making ability of actors. For adults, this self-determination is fully embraced in principle, but for children, the boundaries must be explored on an individual basis due to children's emotional and intellectual immaturity. Currently, individual privacy protection can only be practiced to a limited extent because of statistical and machine learning-based analysis and targeting processes (Roßnagel, 2019; Mühlhoff, 2021). Therefore, especially regarding children and the future, collective and societal safeguards must be taken ("group privacy", see Taylor et al., 2017).

[3] 'IT fundamental right' is a translation of the German colloquial term 'IT Grundrecht'. This short term refers to a ruling by the German Federal Constitutional Court from 2008 which established the fundamental right to confidentiality and integrity of IT systems ("Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme").

Current challenges regarding media and children

That children start using their own digital devices from a young age and that we are facing an increasing mediatization of childhood (Kutscher, 2012; Tillmann & Hugger, 2014) has long since become normal. Current usage figures show that even very young children at the age from 8 to 10 have their own smartphone and access to the internet. In Germany, for example, 94% of 12 to 19-year-olds already have their own smartphone (Rathgeb & Behrens, 2020a), which they use daily for apps such as WhatsApp and YouTube as well as digital games. At the same time, 89% of young people are online every day (Rathgeb & Behrens, 2020a). The most popular apps used by children and young people in 2021 were WhatsApp, Instagram, YouTube, Snapchat, and TikTok (Hajok, 2021). On the platform TikTok, content is not only passively consumed. It is also being created mostly by children themselves in the form of short video sequences in TikTok, content, but short video sequences are also actively created by the young users themselves (Hajok, 2021; Stecher et al., 2020).

In a study that surveyed young people about their privacy behavior, 67% of respondents said they disapproved of these apps storing their personal data (Engels, 2018). However, for the most part, this had no impact on their usage behavior. This phenomenon is referred to and discussed by scholars as the "privacy paradox" (Barnes, 2006; Baruh, Secinti & Cemalcilar, 2017; Norberg, Horne & Horne, 2007). Scholars (Livingstone, Stoilova & Nandagiri, 2019) show this contradictory behavior in how children willingly share personal information on the internet, thereby accepting risks to their safety and privacy, despite wanting to protect their personal data. The contradiction is then that social participation is only possible through giving up conventional notions of privacy. Studies with adult participants also emphasize that a sense of powerlessness, resignation, and lack of choice elucidate this privacy paradox (Matzner et al., 2016; Stoycheff, 2016). Others emphasize that the seemingly contradictory usage behavior is instead about negotiating various moral concepts, which can be more aptly described by concepts of risk analysis rather than paradoxes. Furthermore, through a more detailed analysis based on the psychological "Theory of Planned Behavior", the privacy paradox is shown to only seemingly be a paradox. The theory reveals that when specific inclinations and intentions are inquired about, a congruence of dispositions and privacy-related behavior can be demonstrated (Dienlin & Trepte, 2015). With younger children, there is the additional problem of determining if they have the necessary level of knowledge and experience that would allow them to make these kinds of judgements in the first place.

Popular apps such as Instagram, TikTok, and Snapchat require users to be at least 13 years old, while WhatsApp, for example, raised their age restriction to 16+ with the validity of the GDPR guidelines in May 2018. However, these age restrictions are a mere technicality with no practical significance since these applications are downloadable and accessible without any serious age verification. This then raises the question of whether such a form of self-regulation is a valid instrument for preventing children and young people from using apps with critical data protection features. As the apps do offer many benefits for young people, it does not seem justifiable to prohibit their usage on the grounds that refrainment would entail fewer risks.

The design of social media apps and interfaces systematically employs mechanisms developed in the gambling industry that aim to keep users engaged for as long as possible (5Rights Foundation, 2021; Hagendorff, 2019). In this context, unlike in the gambling one, Shoshana Zuboff (2018) draws attention to the distortions that can arise when the mechanisms in question are applied to children and young people in a largely unregulated manner. As the revelations from the "Facebook Files" in 2021 brought to light, social media is extremely problematic for young people. Instagram, in particular, focuses on body image and has serious effects on teenagers, especially girls, as they are in a phase of becoming more conscious of their bodies (Wells, Horwitz & Seetharaman, 2021). Furthermore, Facebook aims to introduce children to its services before they are formally old enough (Wells & Horwitz, 2021).

Children gain access to digital content, networks, and platforms that enable their rights to information, media access, and participation in new and complex ways. Yet, at the same time, this access affects their personal rights. Considering that digital media is (or can be) used without any form of parental supervision, and that the legal protection of minors from harmful media is being fundamentally challenged by digital transformations, an increasing number of children are exposed to risks that can detrimentally impact their development (Brüggen et al., 2019). Moreover, the sudden acceleration of digitalization induced by the pandemic has had a significant impact on the everyday lives of children (i.e., the digitalization of school environments). The pressure to act quickly during the pandemic promoted the proliferation of various technologies, which in turn made data protection issues more salient (Rau et al., 2021: 1): "data protection is neither anchored as a topic nor as a design principle" in school processes.

The process of intensive data collection, observation, and surveillance is referred to as part of "datafication" (Lupton & Williamson, 2017). Children's data became a "commodity", linked to marketing interests. There are many areas of implementation, for example:

- gaming apps with captology technology (a computer technology that tries to influence an individual's judgment and/or decision-making behavior) (e.g., Pokémon-Go or Candy Crush Saga);
- smart toys used that systematically collect, analyze, and store data (e.g., the i-Que robot, Cloud Pets);
- the use of group chats in school classes that systematically mine data (e.g., WhatsApp);
- disclosing children's location on social media (e.g., TikTok);
- surveillance in family or school settings by tracking apps (e.g., Little Nanny GPS Tracker);
- individualized and profiling educational software (e.g., Quizlet).

These technologies curtail children's rights to an open future and to experience self-determination. This right curtailment is happening in a digital space that is both public and commercially permeated, but often not fully understandable for (Fahlquist, 2015; Forum Privatheit, 2018). To use certain apps and services for free, individuals are often willing to disclose personal data – without being able to grasp the full implications of the supposedly harmless disclosure of information (Engels, 2018). In this context, privacy threats are also often associated with security threats that can lead to real-world assaults on children (e.g., in the case of location disclosure during children's interactions with adults who pose as children). Such interaction risks (which are additional to the content risks that have been the focus thus far) present a new challenge in child and youth media protection. This is currently the subject of extensive research in the field of civil security (see SIKID)[4].

In digital contexts, children's and young people's decisions and practices are influenced by their social environment and, above all, by the behavior exemplified by their parents and peer group (as further elaborated in chapter "Influencing and Protective Factors in Internet Use by Children and Young People"). Children decide whether to share or withhold personal data in a context of networked communication and practices. A recent study (Livingstone et al., 2019) differentiates between *relational* privacy (the "data self" which is a result of one's social behavior online), *institutional* privacy (the collection and analysis of personal data by government, educational, or health institutions), and *commercial* privacy (personal data used commercially for businesses). Regarding the latter, children feel least empowered. From a structural point of view, today's generation of children is the first to have their biographies comprehensively archived on digital platforms. Even the first

[4] Security for Children in the digital World (SIKID): https://uni-tuebingen.de/en/217161

so-called "digital natives" were not confronted with today's data collection imperatives in a comparable way. In contrast, digital corporations will not only have in-depth knowledge of the children growing up today (their habits, preferences, etc.), but they will also have data on their personal development. The (imminent) external usage of such digital biographical archives, motivated by the economies of data collection, must be taken into account scientifically, politically, and in terms of regulation.

3 Children as a particularly vulnerable group

Children and adolescents are described as a particularly vulnerable group. This vulnerability is based on the fact that children and young people differ from adults in terms of their cognitive prerequisites, their lack of prior knowledge and experience of certain social processes, and their age-specific approach to media. In this context, it is the responsibility of (adult) educators as well as legislation and related institutions to protect children and young people. The protection of children and young people is therefore contingent on distributed responsibilities. These multiple dimensions of responsibility for children are at the core of a media-ethical perspective on children's vulnerability in the digital space.

Cognitive requirements

Sonia Livingstone's studies show that children under the age of 11 are typically not mature enough to fully grasp abstract concepts such as "privacy". They are also not necessarily capable of understanding the financial potential of data and its use in profiling (Livingstone et al., 2019). Only beginning in adolescence do young people develop so-called formal-operational thinking (cf. Piaget, 1972). This is the ability to think more abstractly, including developing an understanding of (non-transparent) correlations. Moreover, children in puberty appear to temporarily have a more restricted functioning of various neural circuits than during childhood or adulthood (Powell, 2006). This can further complicate an understanding of, for instance, the potential consequences of online self-disclosure.

Against this backdrop of their incomplete development, children and young people are thus also particularly susceptible to online services that rely on short-term experiences of success, reward incentives, or social rewards. For their part, these services benefit from the collect data profiles of users – both from actively uploaded data and through the passive and non-transparent collection of data on clicks, website visits, and interactions such as likes. Prominent examples of this – in addition to WhatsApp, Instagram, Facebook, Reddit, and Snapchat, which operate via social reward systems – are digital gaming apps such as Pokémon-Go or the video and music app TikTok. The mechanisms of these apps are based on user engagement through repeated push messages, rewards for achieving goals, social networking with other users or players, and providing a stage for self-expression. For younger users, these mechanisms are particularly difficult to identify, and more-so to stop, once the dynamics of use have started. This phenomenon will persist if educators remain unaware of these dynamics and are not able to aid in informing children of the potential threats involved with digital usage.

Lack of experience

Several publications indicate that children and young people are – to varying extents – unaware of the dangers to their privacy and the potential consequences of inadequate data protection (Heeg et al., 2018; Naplavova et al., 2014). When children are asked more explicitly about the dangers they suspect are on the internet, the clear impact of recent years' media presence can be observed: namely, that fears refer primarily to other users and thus, to vertical privacy threats. For instance, one problem that was frequently articulated was cyberbullying, which individuals tried to prevent by restricting the visibility of individual photos, posts, or even an entire profile (Borgstedt et al., 2014). Likewise, the dangers of being harassed by strangers and cybergrooming are present as well, as rigorously described in a qualitative study carried out in nine European countries (Mascheroni, Jorge & Farrugia, 2014; Nennstiel & Isenberg, 2021). In contrast, there is little awareness of the potential dangers of the data economy (Livingstone et al., 2019).

Age-specific approach to media

Children and young people are often thought of as "digital natives" since they have been brought up with the internet. However, critical reflection on the potential impacts and side effects of using information and media technologies needs to be conducted (for a critical assessment of the notion "digital natives", see Genner & Süss, 2017; Prinzing, 2019). In conjunction with the benefits such as a high technical affinity, the de facto everyday use of the internet also means that certain persuasive mechanisms, like being encouraged to subscribe to content and the presence of personalized advertising, are not (or no longer) questioned. They are instead perceived as natural components in the way the modern internet works (Wang et al., 2019).

Children approach new digital technologies primarily from their own reality and experiences. The fact that children learn new games by simply trying them out, without paying attention to information manuals or warning labels, can be particularly problematic. Threats can thus only be recognized retrospectively (Borgstedt et al., 2014). Online applications, in general, make it difficult for users to assess the degree of visibility of their own activities. In fact, the "publicity" of an interaction is determined by the number of actors involved. For instance, a WhatsApp chat between two people is often considered private (Borgstedt et al., 2014). But despite the service's end-to-end encryption, most people neglect that other users could share their private content, that their metadata is being analyzed by companies, or the security risks of photos being stored. Understanding how their data is being processed is often difficult for both children and their parents because of the convoluted phrasing of the terms and conditions. Further, these terms and conditions are primarily addressed to parents as legal guardians, who are not necessarily involved in using the app. Consequently, informed consent cannot be assumed. Given that children also have a right to privacy vis-à-vis their parents, which serves to prepare them for a self-determined life, media ethics must include and evaluate parental involvement with reservations and in consideration of specific age groups.

However, this lack of informed consent leads to a violation of data protection law since a sufficient basis of information is a central prerequisite for effective consent to data processing under Article 7 (1) of the GDPR – in conjunction with Article 8 of the GDPR in the case of children. The only way users can assess the respective risks and benefits to make an informed decision about consent is if they know all the relevant information. Yet, in reality, individual's rarely have all the necessary information to aptly analyze the risks and disadvantages of consent. Often, due to this information asymmetry, the benefits associated with "free" games and apps outweigh the potential risks of data processing, which are not transparently presented by the provider (for further detail on consent, see Forum Privatheit, 2020).

In their media activities, children want to use certain apps and maintain their friendships without differentiating between "analogue" and "digital". This means that children's privacy should be seen as contextual and relational. Consequently, the younger and more inexperienced users are, the more difficult it is for them to protect their data and privacy themselves. Moreover, to do so in an informed and self-determined manner, knowing the possible consequences for them self and others.

4 Factors that influence and protect children and adolescents when using the internet

As already elaborated above, the way in which children and young people use the internet and social media is influenced by their social environment. In this context, it is important to emphasize educators such as parents, teachers, or even role models of the same age. Another determining context is the so-called affordance character of the applications themselves. In the following, we will discuss to what extent individual aspects can reinforce or inhibit the issues involved in data protection.

Influence by caregivers

A strong motivating factor for general internet use, but also for the use of certain apps, is peer orientation. At a young age, children are foremost guided by the examples set by their parents and older siblings. Children use the internet and apps such as Instagram similarly to their parents – even though this often means unrestricted publication of family photos ('sharenting'). Furthermore, children become habituated to the presence and use of technologies that necessarily require the sharing of data. This can refer to the use of home automation (smart home) control apps, the use of virtual assistants such as Alexa or Siri, as well as the use of online services to structure everyday family life (e.g., the tidying app Highscore House).

Especially in the case of specific behavior patterns, parents have a high level of influence on their children. Learning from them as role models, children and adolescents adopt the behavior of their parents, who in many cases know more about online contexts and potential dangers. However, parents are often overwhelmed by the high level of complexity involved in data processing, making an adequate risk assessment also difficult for them (Kutscher & Bouillon, 2018; Manske & Knobloch, 2017).

This diversity of parents' levels of digital literacy and their handling of personal data protection (where socioeconomic differences also have an impact) must also be considered. After all, the way parents approach privacy issues and data protection can strongly influence children's and young people's competences, even for the negative. This lack of privacy literacy among certain (groups of) parents further contributes to social inequalities and digital knowledge gaps (Paus-Hasebrink et al., 2018). In general, it appears that age restrictions for online apps and digital games are understood as mere "pedagogical recommendations" (cf. Hajok, 2019; Röthel, 2021).

Children and young people are confronted with omnipresent and complex media technologies. To be able to use them in a self-determined and empowered way, children must be enabled to actively reflect on their usage. Children need skills and knowledge, (e.g., about the complex tracking procedures of websites and apps) as well as critical judgment. They must be empowered to reflect on the risks associated with data security and make informed decisions about the protection of personal information. Since this knowledge is also deepened through experience, measures of empowerment should be related to concrete contexts, insofar as possible. Additionally, they should pursue the goal of self-determined action via self-empowerment (Stapf, 2020; Stapf et al., 2021b). As many parents lack competency in this area themselves, such measures should primarily be taught by educational institutions (i.e., by schools and teachers) and then deepened in the family context. Consequently, it is important that enough resources are provided for this educational task. This also entails that these issues and skills must be implemented into teachers' schooling along with necessitating a change to the school curricula (Hansen, 2021; Schulz, 2021; Schulze-Tammena, 2021).

Influence by peers

Children and, in particular, teenagers tend to copy their peers' behavior. Being part of a group is perceived of as more important than protecting one's own data. The benefits of communicating with others online (and thus sharing one's own data) are felt immediately, whereas risks such as the pre-filtering of information and products, cyberbullying, or even identity theft are (or can be) recognized much later.

The particular importance of both needing to adhere to group dynamics and of using apps (i.e., Instagram or TikTok) alongside peers to be part of a community through online interaction are central motives for young people's use of media. Since children and teenagers are still in the phase of identity formation, both the influence of others and the relevance of social interaction have a higher significance than for adults. For example, it is common practice to use WhatsApp groups for class communication (Rathgeb & Behrens, 2020a, 2020b). Children and teenagers are therefore powerless in the face of privacy infringing applications, as non-use is not an option due to implicit communication norms (e.g., in the classroom, peer group, or sports club). Opting out would entail a cut-off from social interactions and communications (Engels, 2018).

Personality development varies between individuals and does not depend on a defined age. Since their self-concept is still being established, children and teenagers are very impressionable. They can easily be influenced by the usage behaviors of their peer groups in an impulsive way and without critical reflection.

Due to the age- and experience-related unawareness of adolescents (e.g., regarding possible future consequences of their current actions as well as the long-term nature of some usage decisions), it is important that young people receive special protection (Dreyer, 2018; 2021). In this context, the principles of pre-consideration of privacy in technology design (privacy by design) and the preselection of privacy-friendly settings (privacy by default) are of particular importance (Bieker & Hansen, 2017; Acquisti, Brandimarte & Hancock, 2022). Data protection must be implemented from the beginning of app development. In addition, apps must be preconfigured in such a way that only necessary data is being processed, and only basic functions are activated. For each extension, a separate informed consent by the users or their legal representatives should then be required.

Influence by affordances of applications

Media applications are designed to virtually encourage children to use them without protection. Thus, through the way they are designed, applications clearly emphasize the benefits and rewarding value of participation in social life as well as the availability of information on socially relevant topics. Potential risks of use recede into the background. This increases the willingness of children and teenagers to share private information. Thus, especially in exchange for free use of certain apps and services, they disclose personal data – often without being able to predict the full implication of this supposedly harmless disclosure of information (Engels, 2018). This is in line with the empirically well-documented approach of "privacy calculus" (Culnan & Armstrong, 1999), which shows that a short-term benefit is often prioritized over long-term (less predictable) consequences. However, the corresponding studies refer exclusively to adults and focus strongly on rational considerations, which has brought criticism to the approach. It thus needs to be questioned whether and in what way these rational considerations take place in children. In addition, many applications suggest a certain level of privacy (such as an exchange with friends on Instagram).

Instead, apps should be designed in such a way that the potential risks become more immediately transparent and hence, more assessable for users. This, however, is not likely to be in the interests of providers whose business model is based on the collection and analysis of data. According to the GDPR, providers of applications that process personal data must be transparent and offer intelligible information about the transfer of users' data. This could be achieved by so-called privacy

icons (Holtz, Nocun & Hansen, 2011), which can use symbols to provide an overview of data processing (Article 12 (7) GDPR). Providers must also ensure data protection-friendly default settings (Article 25 (2) GDPR), where users' data is not shared with third parties by default or even publicly viewable. The GDPR has thus led to a significant increase in data protection requirements put in practice – despite the shortcomings that still exist. This is due to the new sanction options that allow for fines in the hundreds of millions. In addition to the sanctioning possibilities of the GDPR, positive incentives should also be created to ensure that manufacturers and providers implement the data protection principles in their systems from the outset. Thus, also providing transparency about data processing and its risks (Bieker & Hansen, 2017; Data Ethics Commission, 2019).

In general, children seem to perceive threats to their online privacy more horizontally (from other users) than vertically (from data processing companies). This is based on their horizon of experience as well as the social stimuli they are exposed to through their peer groups and school contexts (Santer et al., 2021). Moreover, studies show that the requirements of digital privacy are complicated to understand and emotionally demanding for young people (Santer et al., 2021). It therefore makes sense to question at what age children fully comprehend privacy risks and threats in a horizontal direction and, importantly, also in a vertical direction. For example, the age limits for assuming informed consent vary across Europe. Under the GDPR, children must be at least 16 years of age to give effective consent to the processing of their personal data. In Germany and Romania, this age limit also applies at the state level. However, the GDPR allows countries to set a lower age for consent. For example, France and Greece require consent from a parent or guardian for children under the age of 15; Spain, in turn, considers minors to be anyone under the age of 14; and Denmark, Portugal, and Sweden set the age for consent at 13 years old. According to the GDPR (Art. 7), information about the processing of personal data should be communicated in clear and simple terms – not only for adults, but for all users. With regard to data subject rights, there is no distinction between children and adults. Art. 12 (1) first subparagraph GDPR specifies that this applies in particular to information specifically addressed to children. The problems with the provisions of the GDPR relating to children and the associated potentials for improvement have been addressed by Roßnagel and Geminn 2020 (pp. 55–62, 118, 128, 137).

In the UK, an attempt was made to substantiate the regulations of the GDPR in a child-friendly manner. Even after Brexit, the GDPR was largely adopted, although extensive deviations are planned. For example, there is a code specifically for the protection of children on the internet. The UK code entitled "Age Appropriate Design: A Code of Conduct for Online Services" was introduced in September 2020 and had a 12-month transition period until it came into force. The code prioritizes the interests and safety of children in the digital world. It consists of 15 design standards that intend to hold online services accountable to ensure that the way their services use personal data is appropriate for the age of the child, considers their best interests, and respects their rights (Feikert-Ahalt, 2021).

In the US, child protection rights have been established since 1998 under the Children's Online Privacy Protection Act (COPPA). Nevertheless, some US states have stricter requirements than COPPA. COPPA prohibits the commercial collection and reuse of children's data (Santer et al., 2021). However, only children under the age of 13 are covered by these protections. Thus, from 13 onward, children are no longer protected as children, but rather treated as general consumers. It can be assumed that from a media-psychological point of view, this is clearly too young. Thirteen-year-olds have neither the necessary understanding nor the adequate media competence required for a self-determined and responsible handling of their own privacy on the internet. In particular, the growing threats of vertical privacy risks are not known by them. So far, there has been a lack of qualitative as well as quantitative studies on the effect and interaction of age and media education in relation to the handling of privacy. As a protective measure, the Kids Internet Design and Safety Act (KIDS Act) was introduced into the legislative process in the US. It is designed to protect children

in digital environments, especially regarding social media. It aims to prevent discriminatory or harmful algorithms or manipulative design (Lorenz & Schomberg, 2022).

Despite such legislative progress in certain countries, others, such as Indonesia, have not yet developed adequate protection of children's rights in the digital space (Sofian et al., 2021). From a global perspective, there is a need for the standardization of specific children's rights as well as advancing media education. Likewise, it is essential to develop children's media and privacy skills. The mastery of such skills should also become standard for parents and teachers. In taking these measures, we decrease the risks associated with an increasingly digitalized and AI-dominated life.

5 Privacy from a children's rights perspective

The ability to self-determine which of your own private spaces others are allowed to have access to, or what information they are allowed to view or use, is a key human right. Article 16 of the UN CRC[5] stipulates that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation." Since 1989, the UN CRC has explicitly granted children basic rights as subjects. Since this international treaty was ratified and implemented by Germany in 1992, it has been regarded as ordinary law. The UN CRC thus has the status of a federal law and must be adhered to by all state authorities. If it conflicts with another legal provision, the UN CRC does not take precedence, unlike fundamental rights. However, the relevant German fundamental rights – such as the right to informational self-determination – can be interpreted in a manner that coheres with international law. The conflicting national law is then interpreted in the sense of the UN CRC. This means that treaties under international law, despite 'only' having equal status with other laws and not being consider as a priority, are of increased importance in practice.

A perspective focusing on children's rights to informational self-determination is therefore immensely important. The decisive factor here is the view of adolescents as acting subjects, and not mere objects of the protection of those providing care (Grotkamp, 2022). This perspective is sought through four basic principles: (i) the right to equal treatment and non-discrimination, (ii) the prioritization of children's best interests, (iii) the right to life and development, (iv) and consideration for the views of the children (Maywald, 2012). The 54 articles of the UNCRC are superseded by the best interests of the child in Article 3(1): "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

In March 2021, the UN Committee on the Rights of the Child published General Comment No. 25 on the rights of children in relation to the digital world. It offers member states a guide for implementing children's rights in the digital space based on the four principles outlined above. Even though the General Comment is not a binding document but merely contains recommendations, the central statement is that children's rights are also valid in the digital space.

The German constitution already contains laws with similar content, albeit implicitly. The fundamental right to informational self-determination in Article 2 (1) and Article 1 (1) of the constitution apply directly to children and their caregivers. There is an ongoing debate about whether to grant children's rights "more visibility" by including a "fundamental right for children" in the constitution. The coalition agreement of 2017 by the last German federal government already expressed such an objective. However, a corresponding draft bill in March 31, 2021 by the government (Bundestag document no. 19/28138), did not receive the necessary two-thirds parliamentary majority to pass. It proposed that the best interests of children should be taken into account at all times, not only in the case of state action directly affecting the rights of the child. At the same time, primary responsibility of parents would have remained unaffected. Digitalization was not specifically considered at the time of the draft bill. In a way, this would be somewhat contrary to the legal system, as digitalisation, in general, is not explicitly mentioned in the German fundamental rights codified in the constitution. The fundamental rights relevant to digitalization have been created through court rulings and further development of the law by the highest courts in relation to other fundamental rights. Yet, these are interpretations by the courts, and are not explicitly codified in the constitution.

[5] In the UNCRC, "children" are defined as persons from birth to the age of majority (see Article 1 UNCRC).

In short, this is why a change of the constitution to include digital rights of children would be unusual since there are no other digital rights codified within it (see Geminn, 2020, for a detailed discussion).

The current German government again announced adding children's rights to the constitution, including the right to (digital) privacy. This could have an impact on many different areas of life (from school to family and media regulation). The 2021 coalition agreement of the Social Democrats, Greens and Liberals commits to incorporate separate children's rights in the constitution and to strengthen child protection (Coalition Agreement 2021: 94). Whether or not these plans will materialize remains to be seen.

The EU Charter of Fundamental Rights (CFR) also contains explicit rights for children, although not to the same extent as the UNCRC. These rights are established at the constitutional level and not merely in the rank of an ordinary law. According to the first sentence of Article 24(1) of the CFR, "[c]hildren shall have the right to such protection and care as is necessary for their well-being." In addition, all other fundamental rights also apply to children. These include the right to private life under Article 7 CFR and to data protection under Article 8 CFR.

From the perspective of children's rights, questions of privacy also address the well-being of children. Children should be provided with a good and prosperous childhood, equipped with opportunities to attain skills for their adult lives. This requires an interplay of protection, promotion, and participation rights tailored to children's abilities (Stapf, 2020).

As childhood is still considered a developmental phase, which definition of well-being should we be guided by? Children's well-being needs to not only align with the present, but also to their *possible* futures. In this way, we would be taking into account the dimensions of development of children's "evolving capacities" (Lansdown, 2005). This was considered in the General Comment and, as early as 1980, Joel Feinberg speaks of "the child's right to an open future" (Feinberg, 1980).

An open future from a privacy perspective implies, among other examples, special care in dealing with children's data, a right to be forgotten online, and data economy regarding data traces online. Most business models of commercially successful internet platforms are designed to predict and shape behavior (i.e., predictive analytics, nudging, etc.) and, therefore, are diametrically opposed to the principle of an open future (Van Dijck, Poell & De Waal, 2018; Forum Privatheit, 2018; Zuboff, 2019). This reality necessitates an increased need for protection of children online. And it requires, along with children's rights to freedom of information and expression (Article 13 UNCRC), that children can learn to make their own decisions to protect their privacy based on information they can understand. For this to be possible, educational rights for children (Articles 28/29 UNCRC) are written into law. This requires empowerment measures at home as well as at school and in school facilities. In order to protect children and young people (Article 17 UNCRC) in digital contexts, new approaches must cohere with today's conditions of use such as mobility and media convergence. This requires an array of positive offers for children online. For not only do children begin using the internet at an increasingly early age, but due to the conditions of mediatized worlds (Krotz & Hepp, 2012) they can neither practically nor sensibly be excluded from all digital services until they themselves can legally consent.

Another children's right is their right to participation (Article 12 UNCRC). It is the duty of the child's parents to promote their child's interests as trustees (see also Article 24 (3) CFR). This also includes the development and unfolding of the child's personality. Here, appropriate participation in accordance with the child's development stage is required. "States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child" (Article 12 UNCRC, see also Article 24 (1), 2nd and 3rd sentence CFR, Roßnagel, 2020, with further citations).

Taking this right seriously in the digital context includes requirements for media education, media regulation, and university research. Evidence-based media research about children as well as with children can enable measures that promote children's decision-making competencies and their safe acquisition of self-protection mechanisms. In light of current discussions on the inclusion of children's rights in the German constitution, an urgent need for social reflection and discussion is assumed here.

6 Areas of tension: children's privacy in digital contexts

Strengthening the privacy of children in digital environments and enabling optimal conditions for their protection, empowerment, and participation requires consideration of the associated tensions (Stapf et al., 2021b). Beyond legal regulations and measures for media education, further technical preconditions should be taken to protect children. Here, technological innovations are just as necessary as interdisciplinary research as a basis for policymaking. In addition, legal and technical protection measures should be urgently promoted, especially those that address non-transparent storage and dissemination of user data, both nationally and internationally.

- **In order for consent to be effective, relevant information must be presented in a comprehensible way. It, therefore, needs to be adapted to children's abilities and interests:** For example, how should we deal with the fact that important skills for making self-determined decisions are only being developed in early childhood? How would information on data protection for children have to be formulated and visualized to ensure that children can give consent? How does this develop as one matures (e.g., in the case of children who are still very young compared to adolescents shortly before adulthood)?
- **Parental and children's rights need to be taught together:** Children's rights also include the parent´s duty of care. Parents and legal guardians are responsible for teaching key privacy competencies and for enabling the child to participate in the digital space (Croll, 2019). What empowerment measures then become necessary for parents, educators, and teachers? To what extent can care institutions, such as schools, provide privacy-friendly infrastructures? How can the parents' duty of care be reconciled with the growing self-determination of children, especially with regard to the acquisition of competencies and skills necessary for this? To what extent does this affect school tasks and curricula? Likewise, how does it affect the implementation of data protection requirements as a whole and of data protection by design and by default in particular?
- **Protection, participation, and empowerment rights are strongly intertwined, but can also lead to conflicts:** In principle, all children's rights are equally valid. However, children's rights are also often in conflict with each other. For example, increased participation (Article 12 UNCRC) or expression (Article 13 UNCRC) also lead to increased threats to children's protection rights, as in the case of hate speech, cyberbullying, or increased disclosure of data. In cases of legal conflict, procedures of practical concordance become effective at the level of fundamental rights. How can such lines of conflict be meaningfully addressed in a preventive manner for the protection of minors from harmful media? How can this be developed in practice and used as a basis for media education?
- **Tensions between generations:** Children who are currently growing up in mediatized environments are developing a different and ever-changing understanding of privacy in their everyday lives. How can privacy as an important value for liberal democracy be communicated to the current generation growing up? How can we deal with the fact that children are often more competent than their parents in the use and understanding of technology? How, for example, should class chats via messenger services at school be evaluated, especially regarding users under the required age of 16 according to the GDPR and, therefore, in need of parental consent? What does this mean for the assumption of responsibility in assessing possible consequences of technology use and actions in the digital environment?
- **Challenges in the context of the commercialization of childhood:** How can demands for apps with positive impacts be made and incentive systems established in an increasingly

commercialized global market? Not using digital technologies is not a valid alternative. Rather, approaches for empowering children, young people, and those responsible for them should lead to informed decisions being made to safeguard informational self-determination. At the same time, to avoid the individualization of protection claims (Karaboga et al., 2014), it is equally important to provide children with a safe digital communication environment in which restrictions – up to bans – on the commercial exploitation of children's data and restrictive deletion policies are standard. How could product development based on the analysis of children's usage data be regulated in a way that ensures protection against economic exploitation?

7 Conclusions and recommendations

The following recommendations are intended as a first impulse to advance the political and societal discussion on the topic of digital privacy and children (Stapf et al., 2021c):

1) Children's privacy is a guaranteed right, also in the digital world.

The right to determine for oneself which spaces others may enter or which information they may see or use is a human right. Article 16 of the UNCRC also states that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation." The UN Convention on the Rights of the Child (UNCRC), as a treaty under international law, has guaranteed children fundamental rights as subjects since 1989. Since it was ratified and implemented by Germany in 1992, it must also be considered when interpreting national law. The rights of children guaranteed by the German constitution, the EU Charter of Fundamental Rights, and the European Convention on Human Rights must be given greater enforcement and practical relevance in the use of digital technologies. This is also a central political issue in the current discussion about whether to include children's rights in the German constitution. In its current version, the constitution lacks an explicit statement on children´s rights, but the fundamental rights established do also apply to children. By contrast, there are deficits regarding the enforcement of fundamental rights in the context of digitalization. And while this generally applies to adults as well, this lack of enforcement could have a greater impact on children due to their increased vulnerability.

2) The child's right to an open future is bound to the safeguarding of child privacy

From a children's rights perspective, issues of informational self-determination and privacy are designed with children's well-being in mind. It is about enabling them to live a good and prosperous childhood that provides them opportunities and skills for their adult life. This includes ensuring children have a right to an open future. Providers should be required to comply with legal and technical standards that need to be developed. These standards could include regulation that children, in general, must be exempt from personalized advertising and tracking, or a ban on the profiling of children. Another proposal is to regularly delete any data obtained in sensitive contexts, unless this conflicts with a child's best interests. This would be associated with stricter requirements for data minimization and a genuine right for young people to be forgotten online that goes well beyond Article 17 of the GDPR. This would include, for example, all data obtained in the context of an educational app as soon as the child leaves school, combined with a ban on data transfer to third parties during the period of use. Conflicting best interests of the child that speak in favor of the permanent storage of sensitive data of children can exist, for example, in the retention of texts documenting abuse. In general, and especially in the context of children and young people, consideration should be given to a maximum data retention period in order to prevent the development of biographical clones of an individual by powerful data-processing organizations.

Consideration of the special protection needed in dealing with children's data also implies the general exclusion that children consent to the processing of personal data. Exceptions are only conceivable in cases involving highly personal matters, which are also protected vis-à-vis the parents or guardians. This applies, for example, in the context of counseling in an emergency or conflict situation pursuant to Section 8 (3) SGB VIII, in which sensitive data can be collected without the knowledge of the caregivers (in detail Roßnagel, 2020; see Roßnagel & Geminn, 2020 for specific proposals).

3) Measures for the protection of children must always be accompanied by enabling measures

The state, schools, and parents should promote media education and media literacy by informing children about their privacy rights. To this end, children should first learn about the various forms of privacy in digital contexts and learn to adapt them themselves. Even at a young age, children need parents, educators and teachers who are competent in the area of media education. The German government's digital pact should, therefore, focus not only on the purchase of data-protection-compliant hardware and software (data protection by design and default) and the provision of appropriate infrastructures, but also on the didactic and pedagogical promotion of digital skills in educational institutions. With the aim being for children to be able to make informed decisions for themselves and to receive transparent information that they can understand.

4) Incentive systems for data protection by design and by default aimed at platform operators, companies, and educational institutions should be promoted and honored by the government

Self-determination in the digital world should be the standard – and not have to be actively activated by users via privacy settings. This is particularly important when services are also aimed at children or are used by children. At a minimum, it must be simple for children to understand in which context of privacy and publicity they act, and this must be easily recognizable for them during use, (e.g., via auditory messages or feedback ("If you send this, all people who use the same service can see it")) or via visual design. However, such notices must not be of a disturbing nature. Further, children should not be taught that only if there is a notice, there is threat. Children's self-determination in the digital realm should already be thought of during the design process of digital applications. Companies should be provided with government incentive systems so that the implementation of data privacy by design and by default is ultimately a competitive advantage rather than a disadvantage for them.

5) Digitalization is developing rapidly: Ensuring privacy and data protection as human rights requires approaches that are holistic, interdisciplinary, and sensitive to context

The ability to decide what information is and is not shared in certain contexts or with certain people is tied to other fundamental children´s rights. For instance, it is fundamental to personal autonomy and human dignity. Thus, privacy is a prerequisite for many activities and structures of democratic societies. It is a core issue of liberal democracies facing digitalization. Identifying how teenagers experience and understand privacy in the digital world and how this develops over the course of their lives is indispensable for current and future research.

This requires a "holistic child-rights-oriented approach" (Milkaite & Lievens, 2019) in which new regulatory measures are assessed with a particular focus on their impact on the entire scope of children's rights. To advance this, long-term interdisciplinary studies are needed. In particular, we would benefit from inclusive studies that allow children and young people to participate in the shaping of policies and regulations. This would offer further advancement of innovative technical approaches, societal discourses, as well as a sustainable and flexible protection of children and young people from harmful media.

References

Acquisti, A., Brandimarte, L. & Hancock, J. (2022). How privacy's past may shape its future. Science, 375 (6578), pp. 270-272, DOI: 10.1126/science.abj0826.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394.

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

Bieker, F. & Hansen, M. (2017). Datenschutz „by Design" und „by Default" nach der neuen europäischen Datenschutz-Grundverordnung. RDV, 4, pp. 165-170.

Borgstedt, S., Roden, I., Borchard, I., Rätz, B. & Ernst, S. (2014). DIVSI U25-Studie: Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. SI-NUS Institut Heidelberg.

Brown, M. A. & White, J. (2014): Exploring childhood in a comparative context. An

introductory guide for students. Routledge.

Brüggen, N., Dreyer, S., Gebel, C., Lauber, A., Müller, R. & Stecher, S. (2019). Ge-fährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssi-cher handeln. Bundesprüfstelle für jugendgefährdende Medien.

Croll, J. (2019). Das Recht des Kindes auf Privatsphäre in einer digitalisierten Le-benswelt. Frühe Kindheit, 2(19), pp. 24-31.

Culnan, M. J. & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science, 10(1), pp. 104-115.

Datenethikkommission der Bundesregierung (2019). Gutachten der Datenethik-kommission. Oktober 2019. Datenethikkommission. https://datenethikkommission.de/.

Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European jour-nal of social psychology, 45(3), pp. 285-297.

Dreyer, S. (2018). On the Internet, nobody knows you're a kid. Zur (Nicht-)Erkennbarkeit Minderjähriger in digitalen Medienumgebungen. mer-zWissenschaft, pp. 65-78.

Dreyer, S. (2021). Recht auf mein Selbst – Schutzraume kindlicher Entwicklungs-phasen in der digitalen Gesellschaft. In: Stapf, I. et al.: Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend. Nomos, pp. 143-164.

Engels, B. (2018). Datenschutzpräferenzen von Jugendlichen in Deutschland: Er-gebnisse einer Schülerbefragung. IW-Trends-Vierteljahresschrift zur empi-rischen Wirtschaftsforschung, 45(2), pp. 3-26.

Fahlquist, J. N. (2015). Responsibility and privacy – ethical aspects of using GPS to track children. Children & Society, 29(1), pp. 38-47.

Feikert-Ahalt, C. (2021) United Kingdom. In: The Law Library of Congress: Chil-dren's Online Privacy and Data Protection in Selected European Countries. LL File No. 2021-020137 https://tile.loc.gov/storage-services/service/ll/llglrd/2021680641/2021680641.pdf

Feinberg, J. (1980). The child's right to an open future in whose child. Childrens' rights, parental authority, and state power, pp. 123-153.

5Rights Foundation (2021). Pathways: Howe digital design puts children at risk. https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf.

Forum Privatheit (2018). Tracking. Beschreibung und Bewertung neuer Methoden. White Paper. Friedewald, M., Ammicht Quinn, R., Hansen, M., Heesen, J., Hess, T., Krämer, N., Lamla, J., Matt, C., Roßnagel, A. & Waidner, M., eds.: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Creati-ve Commons 2018.

Forum Privatheit (2020): Einwilligung. Möglichkeiten und Fallstricke aus der Konsumentenperspektive. White Paper. Friedewald, M., Ammicht Quinn, R., Hansen, M., Heesen, J., Hess, T., Krämer, N., Lamla, J., Matt, C., Roßnagel, A. & Waidner, M., eds. Schriftenreihe: Forum Privatheit und selbstbe-stimmtes Leben in der digitalen Welt, Creative Commons 2020.

Geminn, C. & Roßnagel, A. (2015). „Privatheit" und „Privatsphäre" aus der Per-spektive des Rechts - ein Überblick. JuristenZeitung, 70(14), pp. 703-708.

Geminn, C. (2020). Digitalisierung und verletzliche Gruppen im Recht. Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV), pp. 254-288.

Genner, S. & Süss, D. (2017). Socialization as media effect. The international ency-clopedia of media effects, pp. 1-15.

Grotkamp, N. (2022). Kinder und Datenschutz. Zeitschrift für das gesamte Fami-lienrecht (FamRZ), pp. 6-11.

Hagendorff, T. (2019). Jenseits der puren Datenökonomie - Social-Media-Plattformen besser designen. In: Ochs, C., Friedewald, M., Hess, T., Lamla, J., eds.: Die Zukunft der Datenökonomie. Medienkulturen im digitalen Zeitalter. Wiesbaden. https://doi.org/10.1007/978-3-658-27511-2_15.

Hajok, D. (2019). Der veränderte Medienumgang von Kindern. Tendenzen aus 19 Jahren KIM-Studie. JMS Jugend Medien Schutz-Report, 42(3), pp. 6-8.

Hajok, D. (2021). Der veränderte Medienumgang von Kindern. Markante Entwick-lungen und Daten zur aktuellen Situation. JMS Jugend Medien Schutz-Report, 44(3), pp. 7-10.

Hansen, M. (2021): Digitalisierung in der Schule – Datenschutz mitdenken. Auf-wachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend, pp. 313-239

Heeg, R., Genner, S., Steiner, O., Schmid, M., Suter, L. & Süss, D. (2018). Genera-tion Smartphone. Ein partizipatives Forschungsprojekt mit Jugendlichen. Generation Smartphone. http://www.generationsmartphone.ch/.

Holtz, L. E., Nocun, K. & Hansen, M. (2010). Towards displaying privacy information with icons. IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, pp. 338-348.

Karaboga, M., Schütz, P., Friedewald, M., Zoche, P., Matzner, T., Mothes, C., Ne-bel, M., Ochs, C. & Simo Fhom, H. (2014). Selbstdatenschutz. White Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/download/selbstdatenschutz-2-auflage-2014/.

Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP (2021).

https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800.

Krotz, F. & Hepp, A. (2012). Mediatisierte Welten: Forschungsfelder und Beschrei-bungsansätze. Springer-Verlag.

Kutscher, N. (2012). Medienbildung in der Kindheit. MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung, 22, pp. 1-16.

Kutscher, N. & Bouillon, R. (2018). Kinder. Bilder. Rechte. Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie. Schriftenreihe des Deutschen Kinderhilfswerkes e. V., 4, pp. 1-97.

Lansdown, G. (2005). The evolving capacities of the child. Innocentil Insights, 5(18).

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

Lorenz, L. & Schomberg, S. (2022). Kids Internet Design and Safety Act: Daten-schutz kindgerecht gedacht. ZD-Aktuell, 01036.

Lupton, D. & Williamson, B. (2017). The datafied child: The dataveillance of chil-dren and implications for their rights. New Media & Society, 19(5), pp. 780–794. https://doi.org/10.1177/14614448166863

Manske, J. & Knobloch, T. (2017). Datenpolitik jenseits von Datenschutz. Stiftung Neue Verantwortung, pp. 1-97.

Mascheroni, G., Jorge, A. & Farrugia, L. (2014). Media representations and chil-dren's discourses on online risks: Findings from qualitative research in nine European countries. Cyberpsychology: Journal of Psychosocial Re-search on Cyberspace, 8(2).

Matzner, T., Masur, P. K., Ochs, C. & von Pape, T. (2016). Do-It-Yourself Data Pro-tection—Empowerment or Burden? Data protection on the move, pp. 277-305.

Maywald, J. (2012). Kinder haben Rechte!: Kinderrechte kennen-umsetzen-wahren. Für Kindergarten, Schule und Jugendhilfe (0-18 Jahre). Wein-heim: Beltz.

Milkaite, I. & Lievens, E. (2019). Children's rights to privacy and data protection around the world: challenges in the digital realm. European Journal of Law and Technology, 10(1).

Mühlhoff, R. (2021). Predictive Privacy: Towards an Applied Ethics of Data Analyt-ics. Ethics and Information Technology, 23, pp. 675–690. https://doi.org/10.1007/s10676-021-09606-x

Naplavova, M., Ludik, T., Hruza, P. & Bozek, F. (2014). General Awareness of Teenagers in Information Security. International Journal of Information and Communication Engineering, 8(11), pp. 3552–3555.

Nebel, M. (2015). Schutz der Persönlichkeit - Privatheit oder Selbstbestimmung, Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht. Zeitschrift für Datenschutz, pp. 517–522.

Nennstiel, S., Isenberg, M. (2021): Kinder und Jugendliche als Opfer von Cyber-rooming. Zentrale Ergebnisse der 1. Befragungswelle 2021. https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Medienorientierung/Cybergrooming/211216_Cybergrooming-Zahlen_Praesentation_LFMNRW.pdf.

Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), pp. 100-126.

Paus-Hasebrink, I., Sinner, P., Prochazka, F. & Kulterer, J. (2018). Auswertungs-strategien für qualitative Langzeitdaten: Das Beispiel einer Langzeitstudie zur Rolle von Medien in der Sozialisation Heranwachsender. Auswertung qualitativer Daten, pp. 209-225.

Piaget, J. (1972). Intellectual evolution from adolescence to adulthood. Human

development, 15(1), pp. 1-12.

Powell, K. (2006). Neurodevelopment: How does the teenage brain work? Natu-re, 442, pp. 865–867.

Prinzing, M. (2019). Eingeboren? Oder nur eingewandert ins Digitale? Warum die Abkehr vom Mythos einer Generation von Digital Natives Voraussetzung einer verantwortungsorientierten Bildungs- und Gesellschaftspolitik ist. Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend, pp. 283-295.

Rathgeb, T. & Behrens, P. (2020a). JIM-Studie 2020. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12-19-Jähriger. Medienpädago-gischer Forschungsverbund Südwest.

Rathgeb, T. & Behrens, P. (2020b). KIM-Studie 2010. Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang Sechs-bis 13-Jähriger. Medien-pädagogischer Forschungsverbund Südwest.

Rau, F., Galanamatis, B., Gerber, L., Grell, P., Konert, J., Rheinländer, K., & Scholl, D. (2021). Datenschutz und informationelle Selbstbestimmung in der Schule. In: Boden, A., Jakobi, T., Stevens, G., Bala, C. eds.: Verbraucherda-tenschutz-Technik und Regulation zur Unterstützung des Individuums, pp. 1-26.

Röthel, A. (2021). Warum Kinder Rechte brauchen. Kursbuch, 56(201), pp. 47-60.

Roßnagel, A. (2020). Der Datenschutz von Kindern in der DS-GVO. Zeitschrift für Datenschutz, pp. 88-92.

Roßnagel, A. & Geminn, C. (2020). Datenschutz-Grundverordnung verbessern – Änderungsvorschläge aus Verbrauchersicht. Baden-Baden.

Santer, N. D., Manago, A., Starks, A., & Reich, S. M. (2021). Early Adolescents' Perspectives on Digital Privacy. Algorithmic Rights and Protections for Children, PubPub.

Schulz, A.D. (2021). Datenschutz und Medienbildung – Chancen und Barrieren in der schulischen Praxis. Aufwachsen in überwachten Umgebungen: Inter-disziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Ju-gend, pp. 279-292

Schulze-Tammena, R. (2021). Wie kann Schule einen Beitrag zur Entwicklung „digi-taler Mündigkeit" bei Kindern und Jugendlichen leisten? Die Herausforderung der Schule als medienpädagogischer Lernort für Datenschutz und Da-tensparsamkeit. Aufwachsen in überwachten Umgebungen: Interdiszipli-näre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend, pp. 237-254

Sofian, A., Pratama, B., Besar, F. C. P., & Capaldi, M. P. (2021). Original Paper, A Brief Review: Children Online Privacy Protection in Indonesia.

Stapf, I. (2020). Aufwachsen in überwachten Umgebungen: Medienethische Über-legungen zum Kinderrecht auf Privatsphäre im Zeitalter des Digitalen. Aufwachsen in überwachten Umgebungen – Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend.

Stapf, I., Ammicht Quinn, R., Friedewald, M., Heesen, J. & Krämer, N., eds. (2021a): Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend. Baden-Baden.

Stapf, I., Ammicht Quinn, R., Friedewald, M., Heesen, J., Krämer, J. (2021b): Aufwachsen in überwachten Umgebungen: Privatheit von Heranwachsenden als ein neues interdisziplinäres Forschungsgebiet (Einleitung). Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privat-heit und Datenschutz in Kindheit und Jugend.

Stapf, I., Meinert, J., Heesen, J., Krämer, J., Ammicht Quinn, R., Bieker, F., Friedwald, M., Geminn, C., Martin, C., Nebel, M., Ochs, C. (2021c): Das Recht von Kindern und Jugendlichen auf Privatheit in digitalen Umgebun-gen: Handlungsempfehlungen des Forum Privatheit, Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend, pp. 351-376.

Stecher, S., Bamberger, A., Gebel, C., Cousseran, L., & Brüggen, N. (2020). "Du bist voll unbekannt!". Selbstdarstellung, Erfolgsdruck und Interaktionsrisi-ken auf TikTok aus Sicht von 12-bis 14-Jährigen. Ausgewählte Ergebnisse der Monitoring-Studie. München: JFF-Institut für Medienpädagogik in Forschung und Praxis.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. Journalism & Mass Com-munication Quarterly, 93(2), pp. 296-311.

Taylor, L., Floridi, L. & van der Sloot, B., eds. (2017). Group Privacy: New Challeng-es of Data Technologies. Springer.

Tillmann, A. & Hugger, K. U. (2014). Mediatisierte Kindheit–Aufwachsen in media-tisierten Lebenswelten. Handbuch Kinder und Medien, pp. 31-45.

Van Dijck, J., Poell, T. & De Waal, M. (2018). The platform society: Public values in a connective world. Oxford University Press.

Wang, X., Shi, W., Kim, R., Oh, Y., Yang, S., Zhang, J. & Yu, Z. (2019). Persuasion for Good: Towards a Personalized Persuasive Dialogue System for Social Good. arXiv preprint arXiv:1906.06725.

Wells, G. & Horwitz, J. (2021): Facebook's Effort to Attract Preteens Goes Beyond Instagram Kids, Documents Show. https://www.wsj.com/articles/facebook-instagram-kids-tweens-attract-11632849667.

Wells, G., Horwitz, J. & Seetharaman, D. (2021): Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show. https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

PROJEKTPARTNER

Fraunhofer

Natur
Technik
Kultur
Gesellschaft
UNIKASSEL VERSITÄT

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

INTERNATIONALES ZENTRUM
FÜR ETHIK IN
DEN WISSENSCHAFTEN