



FREuDe

JEAN MONNET CENTRE OF EXCELLENCE
COMMUNICATION, FACTS & REGULATION FOR EUROPEAN DEMOCRACY

mediagov@univie.ac.at 

Währinger Str. 29, A-1090 Wien 

mediagovernance.univie.ac.at 

POLICY BRIEF

August 2023

PROACTIVE AND OPTIMAL PROTECTION OF CHILDREN'S DIGITAL PRIVACY AS THE CORNERSTONE FOR EUROPEAN DEMOCRACIES

Oleksandra Gudkova

Katharine Sarikakis

Who is this aimed at

- policymakers, government authorities, industry stakeholders, educators, parents, and guardians in the EU

Key messages

- Children's rights are inextricably connected to the right to privacy in the digital world both because the right to privacy is a human right and because privacy is essential to democratic practice and citizenship.
- The EU must take further proactive measures to safeguard children's digital well-being as a right to social, cultural, economic and political citizenship, addressing the digitalisation and storage of children's learning data, identity theft, unregulated sharing of children's data online, as well as data related to online behaviour.
- Parents, guardians, teachers and carers, but importantly industry, and EU authorities have a crucial role in empowering children as citizens by proactively protecting privacy, certain forms of anonymity and online civility..
- The EU and national states must require an ethical governance protocol that includes optimal proactive and responsive methods in technological design and use which protects and empowers children with the aim of maximum self governance and determination of their own content

Introduction

"Today's children are the first generation to be born into a digital age, while their parents are the first to rear 'digital' children... Threats to children's privacy, both in the digital space and out of it, are increasing at alarming rates. Parents have a role to play in protecting their children's right to privacy, but it is not only up to them. States must safeguard children's rights by establishing appropriate practices and laws, and also ensuring information is available to children themselves on exercising their rights."
(UN OHCHR Report, 2021)

Internet users are subjected to a number of threats concerning their personal data and other information that is being collected when they spend time on social media platforms. The importance of privacy as a human right has been re-assessed in practice and policy over the past decade repeatedly, due to the pressures its exercising undergoes under the global system of media platforms and the intrusive strategies of states. Not only is privacy as a right increasingly determined by global media platforms, but also even state authorities when not violating this right, operationalise its protection by limiting its scope. As is the case with the GDPR European Union legislation for the protection of personal data, privacy is concretised as a question of personal data. Children have a special mention in EU law as they can be considered particularly vulnerable and in need of additional measures of protection. This policy brief emphasises the significance of ensuring children's rights to digital privacy and identity protection in the European Union, providing practical recommendations to create a secure online environment for young individuals.

State of the problem and European legislative status quo

According to the UN report presented to the Human Rights Council in 2021 on digital privacy and children's privacy, children's use of social media doubles between the ages of nine and 12, with some 40 percent of them having multiple social media profiles. On average, a teenager's online contacts double during secondary school.

Just as much as children are exposed to the vast digital landscape, the digital landscape exposes children to potential risks and violations of their rights, in particular regarding digital privacy and identity protection. Moreover, everyday activities and spaces where children develop, such as learning and schooling, family time and private sphere, become objects of digital content in the form of personal data- from identification issues such as age, gender, ethnic and economic background to images of and information about personal moments and matters through parental social media sharing. "Child's digital identity commences before birth with in-utero images shared by parents and families across the web, many of which are embedded with personal information. Some 80 percent of children living in developed Western countries have a digital footprint before they are two years old, largely due to the actions of their family members." (UN OHCHR Report, 2021). In these cases, children are left largely disempowered to act on their own interests. In the world, each year, over one million families suffer from children's identity fraud. In the EU Kids online 2020 survey on benefits and challenges in the digital world, carried out among children aged 9–16 from 19 European countries, respondents indicated that some of the biggest challenges online, among others, were unwitting personal data collection, identity theft, fraud and blackmail leading to one in 10 children never feeling safe online.

Hence, it is not only children's online presence increasing daily, but also the conditions forcing children to partake in digital activities are increasingly pressurising, so that it becomes essential to address these challenges and develop comprehensive policies to safeguard children's digital well-being while acknowledging and protecting their human rights.

The three main issues requiring proactive attention are:

1. Digitalisation and Storage of Children's Learning Data

Children's learning data refers to the information generated from their online activities, such as how they think, learn, engage with content, respond to stimuli, and share the content they consume.

a. Lack of awareness: Children may not fully understand the implications of sharing their learning data, and they may not be aware of how this information can be used by online platforms and educational services. Children generally have a particularly limited understanding of the collection and processing of their personal data by commercial actors, narrowed to "Google knows my favourite music" or "Gmail sees my name and password" (Livingstone et.al., 2022).

b. Lack of choice and exclusion: it cannot be assumed that children or families have a real choice when it comes to whether and which learning platforms and software is to be used, as those decisions are taken solely by schools or educational authorities. Even in rare cases of withdrawal from usage of a particular platform, this translates in disadvantage for learners.

c. Data breaches: Educational platforms that collect and store children's learning data may be vulnerable to data breaches, leading to the exposure of their sensitive information to unauthorised parties.

d. Profiling and targeting: Analyzing children's learning data can lead to the creation of detailed profiles, which may be used for targeted advertising or other purposes without their consent.

2. Identity Theft

a. Limited knowledge: Children may not be aware of the warning signs of identity theft or understand the importance of safeguarding their personal information.

b. Parental oversharing: Parents sharing their children's personal information and images on social media without adequate privacy settings or awareness of the right of children to privacy, in particular in the right of digital footprints of usage and exposure online, may expose children to identity theft risks.

c. Misuse of information: Stolen personal information can be used to open credit accounts or take out loans in the child's name, leading to long-term financial consequences that may only become apparent later in life.

3. Unregulated sharing of children's data and images by their parents and guardians

a. Lack of consent: Children, depending on their age, can or may not have the ability to give consent for their information or images to be shared online, leading to potential violations of their privacy rights.

b. Digital Footprint: Children's digital footprints start forming from a very young age due to parental sharing, creating a vast trail of information that may be difficult to control or erase in the future. Some parents go to the extent of creating social media profiles for their children before they are born.

Recital 38 of EU GDPR on Special Protection of Children's Personal Data states that *"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counseling services offered directly to a child."*

Recital 38 forms the basis of the special mention of the protection of children under the European Directive for the protection of personal data, under Article 8:

- 1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old.*
- 2. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.*
- 3. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*

The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

In 2022, European Commission adopted a new European strategy for a **Better Internet for Kids (BIK+)**, to improve age-appropriate digital services and to ensure that every child is protected, empowered and respected online. Currently, The EU is in the process of replacing its ePrivacy Directive with an **ePrivacy Regulation**. Depending on any new provisions this Regulation has, it may have implications for the protection of children online. Further, initiatives such as **Insafe**, a network supported by the European Commission to implement awareness-raising campaigns on e-safety at national level, are of crucial importance.

The Council of Europe has also published an **Internet Literacy Handbook**. Research on children's vulnerabilities on the net should be further supported in order to increase the effectiveness of education tools.

Policy recommendations

Empowering parents/guardians and educators

While there are several actions open to governments, protecting children's privacy has become, in part, a task for educators, newly charged with explaining the digital world to their students so that they can, supposedly, protect themselves. From the basics of access to and operation of devices through to a critical grasp of how personal data is processed, digital literacy is crucial to inclusion, equality and other rights in a digital age. (Livingstone et.al., 2022)

The EU's GDPR provides that consent from a parent or legal guardian must be provided to enable companies to process personal data for children under 16 years of age. Other than requiring consent, there is a need for specific guidelines for parents and guardians on best ways in which to protect their children's data online and help them make smart choices about what they share about themselves and others.

These should include but not be limited to talking to children about their online reputation and teaching them privacy. Numerous websites that appeal to children often request them to disclose personal information, such as pictures of themselves and their friends, their names, addresses, and preferences for music, films, and games. Others, such as applications do not even have privacy policies (van der Hof and Lieven 2018). While these platforms allow them to foster relationships and share their interests, it is crucial to engage in conversations with children to ensure they comprehend the potential risks associated with oversharing online.

It is crucial to teach children how to review privacy settings on social networks, encourage them to manage passwords, clean up apps on devices, be careful who they share their personal data with, and teach them about things like identity theft and harmful information.

Recommendations for families to help reduce the risks of child identity fraud:

- keep personal information private, online and on paper;
- do not share your children's information on social media;
- set positive online examples for your children by practicing safe online behaviours yourself;

limit and monitor the use of social media and messaging platforms;

- monitor your child's online activity, particularly as it relates to potential cyberbullying;
- platforms that allow users to direct/private message (DM), friend, or follow other users via public search pose the greatest concern;
- enroll in an identity protection service. (Javelin Strategy & Research, 2021).

Developing a unified EU Children's Digital Privacy and Identity Protection Act

The EU must establish comprehensive and harmonised regulations specifically tailored to protect children's digital privacy and identity across all member states. Age of consent has been deemed to be a national matter and not below the age of 13. Neither of these approaches is helpful as children well under the age of 13 are active on social media while the differences in age of consent provide an environment where children of rather great development differences due to age are assumed fully responsible for online behaviours. There is a clear need for specific guidelines and thresholds on data collection, age-appropriate consent mechanisms, proactive protection of minors and mechanisms to rectify data breaches.

Encourage online platforms and technology companies to implement robust privacy-by-design principles, age verification measures, and user-friendly settings to safeguard children's personal information and ensure they have age-appropriate experiences online.

Safeguarding children's rights to digital privacy and identity protection is of utmost importance in the European Union. By implementing these policy recommendations, the EU can create a safe and secure online environment for its young citizens, empowering them to explore the digital world while minimising potential risks and violations of their rights.

Monitor and require from platforms and software companies where children are particularly active to revise and develop safety net systems, educational and information supportive programmes, develop privacy safety features as standard for children use, provide explanation of terms and conditions in suitable language and allow a technological architecture that maximises personal choice and self governance of personal data, including true delete functions.

References

Better Internet for kids. Review of the year 2022.
https://www.betterinternetforkids.eu/documents/167024/184597/BIK_Report2022_WEB.pdf/b18efc2c-8726-5290-d51b-fddfd00cd19?t=1675761162691

Council of Europe. Protecting children's rights in the digital world: an ever-growing challenge.
<https://www.coe.int/ti/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1>

Council of the European Union. European strategy for a Better Internet for Children, May 2012.
https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/educ/133824.pdf

EU GDPR. <https://gdpr-info.eu/>

Internet matters. Protecting your child's data.
<https://www.internetmatters.org/issues/privacy-identity/protect-your-childs-data/>

Livingstone, S., Bulger, M., et.al. (2022) Children's privacy and digital literacy across cultures: Implications for education and regulation. in Learning to Live with Datafication : Educational Case Studies and Initiatives from Across the World. Pangrazio, L. & Sefton-Green, J. London: Routledge

Javelin Strategy & Research (2021) Child identity fraud: a web of deception and loss. Report.
https://javelinstrategy.com/sites/default/files/files/reports/21-5012J-FM-2021%20Child%20Identity%20Fraud%20Study_1.pdf

Milovidov E., Richardson J., Schmalzried M. (2017) Internet literacy handbook. Council of Europe.

Smahel, D., Machackova, et al. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo

The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights (2021) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement>

United Nations Human Rights Office of the High Commissioner. Children's right to privacy in the digital age must be improved <https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved>

van der Hof S., Lievens E. (2018) The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR . Communications Law Vol. 23, No. 1, Available at SSRN: <https://ssrn.com/abstract=3107660>

The Policy Brief is published in the framework of the FREuDe project. The project aims to intervene for positive future social change that derives from the commitment and intellectual input across disciplines, such as Sociology, Law, Education, Childhood and Youth studies, European studies and Politics, as well as Communication scholarship and Security studies. Moreover, the Centre addresses the question from the perspective of future autonomous citizens, today's children, and explore closely the ways in which information and Europe feature in their lives.

Jean Monnet Communication, Facts and Regulation for European Democracy (FREuDe) Centre of Excellence

- stimulates new forward thinking with regards the role of facts and place of regulation for securing a future democratic Europe
- generates new research and policy-oriented thinking about integration on the basis of informational rights and enabling informational environments across disciplines not traditionally involved in studying Europe:
- develops new agendas for research, policy and teaching across disciplines and across stakeholder communities
- provides an impetus for future oriented thinking, by researching the needs and perceptions of Europe's future autonomous citizens, young people and in particular children for factual information in and about Europe
- mobilises knowledges and competencies of a range of experts and especially aiming to "hear from" stakeholders which have historically been permitted least input to questions of right to accurate and comprehensive information as a civil and human right.

Oleksandra Gudkova is a senior researcher at the Jean Monnet Centre of Excellence FREuDe, Media Governance and Industries Research Lab, Department of Communication, University of Vienna, Austria

Katharine Sarikakis is a Professor of Communication Science at the Department of Communication, University of Vienna. Prof. Sarikakis leads the Media Governance and Industries Research Lab and is currently the director of Jean Monnet Centre of Excellence FREuDe.