COMMERCIAL EXPLOITATION OF CHILDREN AND ADOLESCENTS ONLINE

How to ensure a rights-respecting digital childhood

FORBRUKERRÅDET

November 2024

Cover page: VON Kommunikasjon

Table of contents

Summary

Children and adolescents rely on digital services for many aspects of their lives. The internet has provided new ways to communicate and build relationships, express themselves creatively and politically, seek knowledge, and much more. However, the dark sides of internet use have grown in tandem with the mass adoption and normalization of online life. Young children are exposed to disturbing and toxic content, adolescents are bombarded with commercial practices that preys on their vulnerabilities, and excessive screentime interferes with offline life.

Policymakers have a responsibility to protect citizens, whether they are young or old. Businesses also have a duty to respect children's rights. Over the past 20 years, there has been a failure to handle the harmful sides of digitalization. As awareness about the harms of social media platforms grows, politicians and regulators are looking for solutions.

This report aims to map the main harmful effects of online life – and particularly social media use – on young people, to create a basis for further discussions about which measures can and should be implemented to reduce these effects. While the report primarily maps out these harms through a consumer lens, other harmful effects are touched upon where it is necessary to get a more holistic overview of the risks faced by young people online.

There are many ongoing debates among both policy makers, governments and regulators, about the introduction of hard technical measures to block or remove children and adolescents from certain digital services. The report provides an overview of key shortcomings of this approach, as well as the many risks that the use of ID-based age verification solutions introduce to children and adults alike.

The report concludes with a number of policy, regulatory, and technical measures that can be implemented to address the harmful effects of online life. We believe that such measures can help pave the way for a safer and healthier internet for everyone, without resorting to invasive or exclusionary measures.

The measures can broadly be summarised to demand a better internet for children and youth by:

1. **Holding the companies accountable,** to remove their addictive mechanisms, use recommender systems that empower individuals instead of amplifying toxic content, and stop illegal advertising practices.

2. Rigorous, coordinated and dissuasive **enforcement of existing rules** and regulations at the national and international level.

3. **Targeted updates of consumer law** where existing rules and enforcement are not sufficient. This includes horizontal protection for all consumers, where this provides the strongest protections for children, in addition to special protections for children.

4. **Only using age assurance if it is in accordance with a number of principles** designed to protect rights such privacy, access to information and participation.

5. **Providing clear guidance for** parents, caregivers, and children, including recommended age limits for social media platforms.

The report was finalized 1 November 2024.

1. Introduction

The internet in general, and digital platforms in particular, has had significant effects on consumers, individuals, and society at large. For individual consumers, platforms such as social media services are an important part of day-to-day life. It is where we organize our lives, communicate with friends and family, go shopping, keep up with news and events, and much more.

At the same time, many technology companies use their platforms to extract 'value' from their users. Fuelled by the financial incentive to show advertising, sell products, and collect personal data, digital services such as social media platforms are designed to keep people scrolling and interacting as long as possible, and by any means. This has contributed to a widely criticized toxic online environment, where gigantic technology companies deploy armies of engineers, designers, psychologists, social scientists and lawyers[1] to create addictive experiences that feed on outrage, fear, insecurities and hatred.

Although the addiction-driven outrage-machines that many online platforms have become have significant negative effects on all consumers, the harms become particularly insidious when the subjects are children. Their experiences online have received too little attention, in part because they are hidden by personalised digital services and small screens, which makes it difficult for parents, caregivers and other adults to keep track of what is going on. The proliferation of children and adolescents on what are essentially digital advertising platforms is controversial and of major concern to parents and caregivers, policymakers, society, and in many cases to the children themselves.[2]

There are countless examples of young children being exposed to toxic content such as suicidal ideation and brutal violence, aggressive advertising related to products for weight loss and cosmetic surgery, and a wide array of other deeply problematic practices.[3] Digital services are designed for engagement at all costs, without regard for how this affects users' autonomy, rights, self-confidence, and mental wellbeing.[4] Children themselves often lack the faculties

[1] "Ex-Google CEO says successful AI startups can steal IP and hire lawyers to 'clean up the mess'", Alex Heath, The Verge (2024). https://www.theverge.com/2024/8/14/24220658/google-eric-schmidt-stanford-talk-ai-startups-openai

[2] "Pathways: How digital design puts children at risk", 5Rights Foundation (2021). https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf.

[3] See for example BEUC's complaint against TikTok from 2021: "BEUC files complaint against TikTok for multiple EU consumer law breaches", https://www.beuc.eu/press-releases/beuc-files-complaint-against-tiktok-multiple-eu-consumer-law-breaches and their position paper on influencer marketing: "From influence to responsibility - Time to regulate influencer marketing" (2023), https://www.beuc.eu/position-papers/influence-responsibility-time-regulate-influencer-marketing.

[4] "Disrupted Childhood. The cost of persuasive design", 5Rights Foundation (2023). https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf

and abilities to process and deal with many of these issues, and the wide systemic and complex mechanisms at work mean that parents and caregivers also often feel completely helpless in the struggle against big tech companies.

This report argues that many of the harms to which children are exposed on digital services are closely linked to the dominant, predatory business models online. It involves the use of addictive mechanisms, deceptive design patterns, and the amplification of toxic content. There are some harms that fall outside the scope of the consumer lens – but are also linked to the business models of the platforms – such as mental health harms, cyberbullying, unwanted interactions with strangers, and sexual exploitation. The report touches upon these issues, but not extensively, due to the Norwegian Consumer Council's mandate as a consumer organisation.

1.1. A better online environment for young people

The public debate about how to protect children and young people online is often concentrated on how to keep young people completely away from services such as social media platforms. While keeping children and adolescents safe is an important and laudable goal, and not all platforms should be accessed by children, this approach is inherently restrictive and inevitably involves many significant downsides.

We believe that there are other approaches to addressing the harms of online platforms that do not preclude young people from all participation. The foundation of this belief is an idea that the internet and services such as social media are not inherently harmful technologies, and that it is possible and desirable to envision a better digital world.

As we will explore further in the report, children and adolescents have the right to access technologies that allow them to interact with each other, engage with topics and causes they care about, and receive information that is important to them. However, technology companies have made these things dependent on also accepting mass-scale commercial surveillance, exploitative algorithmic recommender systems, and aggressive marketing strategies, essentially using children as test subjects for the massive behavioural experiments of Silicon Valley and its ilk.

Although the dominant online platforms are currently tightly entrenched with toxic algorithms, intrusive surveillance and tracking, deceptive design patterns, and illegal content, these negative aspects are not fundamental features of the services. We believe that companies can be forced to design platforms – or part of their platforms – in ways that are conducive to positive, safer, and empowering experiences for children and adolescents.

A better digital environment for children and adolescents does not necessitate their total exclusion from social media and other digital services. Rather than focusing on how to keep people from accessing digital services, the onus should be on companies to take responsibility and accountability for the services that they provide. History has shown repeatedly that this will not happen without significant regulatory intervention and effective enforcement.

Many of the problematic aspects commonly associated with children's internet usage are not exclusively tied to digital spheres. Phenomena such as bullying, mental health deterioration and attention deficiency may have complex and multifaceted causes that cannot solely be attributed to the use of technologies. It is too simplistic to assume that the solution to social and structural issues can or should be solved through technological means such as age verification schemes. Some technological measures may help alleviate symptoms of broader problems, but these should not be considered in a vacuum.

Rather than focusing on apparent silver bullets and one-size-fits-all solutions, there is an urgent need for a variety of measures that work cumulatively toward ensuring better and safer experiences online for everyone. Digital service providers should be forced to design their services in line with human rights obligations and according to applicable laws. Consumers of any age should be allowed more control over what content they are exposed to, and how much and when they use digital services. No companies should exploit children's vulnerabilities to target commercial messaging at them.

Children of a broad range of ages should be empowered by digital services. This requires a fundamentally rights-respecting approach to the development and management of digital services, but also age-appropriate design that accounts for young people's different capacities and needs for protection. However, self-regulatory and individualized self-help measures are clearly insufficient, and must be replaced by strong regulation, policy measures, and robust enforcement.

1.2. About the authors

The Norwegian Consumer Council is a publicly funded, independent consumer organisation that represents consumer interests. We receive no funding from private companies.

This report was written with contributions from BEUC, EDRi, 5Rights Foundation, Anja Salzmann (post-doc at the Centre for the Science of Learning and Technology (SLATE) at the University of Bergen), Jürgen Bering (Head of Center for User Rights at Gesellschaft für Freiheitsrechte), and Jon Worth.

2. How do children's rights apply to the digital environment?

Any person under the age of 18 is considered a child and has rights under the UN Convention on the Rights of the Child.[5] All the EU and EEA member states are party to the Convention, which means they must ensure that children have sufficient protections and rights in accordance with the Convention, online as well as offline. This can for example be done through legal or political means. The rights recognised as applicable to all children are elaborated for the digital sphere in the UN General comment no. 25 on children's rights in relation to the digital environment.[6]

States should not allow commercial actors to exploit or unduly influence children,[7] for example through advertising, targeted commercial content based on profiling, or commercial tracking and profiling of children. This includes protections against deceptive design practices, for example design that can create a false sense of trust and connection,[8] or design that pushes children to spend more time or money than intended. Protections against commercial influence is crucial to empower children's rights in a variety of ways, to support their autonomy, freedom of expression and thought, right to leisure and play, and right to education.

In practice, digital services must be designed and managed considering the best interest of every individual child, as well as groups of children.[9] This is particularly important if digital services place children's different rights in apparent tension, or if other party's interests are in conflict with the child's interest. For example, if there are conflicts between companies' commercial interests and the best interest of children, the best interest of children should prevail.[10] Ensuring the best interest of every child includes age-appropriate and non-manipulative measures that consider the age and state of development of the child. Data protection, privacy-by-design and safety-by-design approaches are important tools for this purpose.[11]

---

[5] "Convention on the Rights of the Child", United Nations (1989). https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.
[6] "General comment No. 25 (2021) on children's rights in relation to the digital environment", United Nations. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[7] General comment No. 25 (2021) para 40-42.
[8] "Dark Patterns of Cuteness: Popular Learning App Design as a Risk to Children's Autonomy" in "Children, Young People and Online Harms", Stockman, Nottingham (2024). https://link.springer.com/chapter/10.1007/978-3-031-46053-1_5.
[9] General comment No. 25 (2021) para. 12.
[10] For a thorough analysis of the best interest of the child, see "The best interests of the child in the digital environment", Livingstone, Cantwell, Özkul, Shekhawat, Kidron (2024). https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf.
[11] General comment No. 25 (2021) para. 110.

Children have the right to non-discrimination, which encompasses equal and effective access to digital environments in ways that are meaningful to them. States are bound to take 'all measures necessary to overcome digital exclusion'.[12] Discrimination can also occur in the form of cyberbullying, or if algorithmic systems based on biased data, code or profiling are used to make decisions concerning the child.

Children also have the right to privacy and to the protection of their personal data, through the integration of privacy-by-design in services they use.[13] This includes that they are entitled to protections against monitoring and intrusive tracking by both commercial and state entities. As a child grows older, parents or caregivers should allow them increasing autonomy and privacy.[14] The right to privacy is closely linked to the right to freedom of thought and the freedom of opinion. Children must be able to learn, grow and play in environments that do not collect data about them to exploit their emotions and vulnerabilities, and influence them for commercial purposes.[15]

The UN Convention on the Rights of the Child recognises the right of the child to the highest attainable standard of health. The online marketing of product which have a clear impact on children's health (unhealthy food, alcohol, gambling, etc.) has major implications for the fulfilment of this right. The right to health also pertains to practices that may harm their mental health, such as unhealthy engagement in digital games or social media.[16]

States that are party to the UN Convention, are required to ensure companies' accountability. For example, States must ensure companies comply with children's rights requirements, offer children, parents and caregivers effective remedies, and should encourage public, timely and accessible information to support children's safe and beneficial use of digital services.[17] Companies should also be required to undertake child rights impact assessments and disclose them to the public.[18]

The UN General Comment on children's rights in the digital environment emphasizes that while children must be protected in digital settings, the use of digital services can be crucial to children, including for social interaction and development, education, autonomy, having their voices heard, and to help them

[12] General comment No. 25 (2021) para. 9.
[13] General comment No. 25 (2021) para. 70.
[14] General comment No. 25 (2021) para 85.
[15] General Comment No. 25 (2021) para 62.
[16] General comment No. 25 (2021) para. 96.
[17] General comment No. 25 (2021) para. 36.
[18] General comment No. 25 (2021) para 38, see also an example of this here: "Wikimedia Foundation Child Rights Impact Assessment", Wikimedia Foundation (2023). (https://upload.wikimedia.org/wikipedia/commons/d/d8/ArticleOne_-_WMF_Child_Rights_Impact_Assessment_Report_2023.pdf).

in times of crisis. States are encouraged to consult with children, for example when developing legislation and policies that affect children's rights.[19]

2.1. Children and adolescents' heterogeneity must be taken into account

Many of the harms outlined in this report are deeply problematic for adults, not only children. None the less, there are many reasons why children's rights warrant additional scrutiny and protection.

Children are in a phase of life where their personalities, opinions and beliefs are being formed. When companies target them with commercial messaging or expose them to toxic content, children may be particularly impressionable. For example, children may struggle to separate advertising from other, non-commercial communication.[20] This makes protecting children from undue influence from commercial actors especially important.

Children's ability to change a lot and quickly also makes violations of their privacy and data protection particularly insidious. As they develop, many children explore and try out different styles, opinions, and interests. They must be allowed to do this, without a log of all their online actions following them for the rest of their lives, to affect them in unknown and incomprehensible ways. Their possibility to explore and change is challenged when companies put them under constant, digital surveillance.

Even through there are certain common traits that make children particularly vulnerable, they should not be considered a uniform entity. Just like adults are different, children vary within and across age groups. Their capacities evolve gradually,[21] and their vulnerabilities vary across socio-economic background, gender, nationality, emotional stability, interests, domestic situations and more.[22] Harmful effects of social media use also differ between individual adolescents.[23] Certain children and adolescents face additional risks because they belong to marginalized groups, for example if they are part of the LGBTQ+ community.

---

[19] General comment No. 25 (2021) para 16.
[20] "Comparing children's and adults' cognitive advertising competences in the Netherlands", Rozendaal, Buijzen, Valkenburg (2010). https://www.researchgate.net/publication/232995879_Comparing_Children's_and_Adults'_Cognitive_Advertising_Competences_in_the_Netherlands.
[21] General comment No. 25 (2021) para 19.
[22] "Changing the odds for vulnerable children", OECD (2019). https://www.oecd-ilibrary.org/docserver/23101e74-en.pdf?expires=1725998095&id=id&accname=guest&checksum=D473DA5CB7A96677F7A56AD6A5103CB6
[23] "The effect of social media on well-being differs from adolescent to adolescent", Beyens, Pouwels, Driel, Keijsers, Valkenburg (2020). https://www.nature.com/articles/s41598-020-67727-7

Some protective measures can have a positive effect on the rights of every child, such as a high level of data protection. Companies providing digital services to children should abide by the data protection principles. For example, they should only process children's personal data in fair and lawful ways, for specific purposes, and minimising the personal data used for these purposes.[24] In practice, abiding by the data protection principles would ensure that children's personal data is used in a very limited way, contributing to important merits like privacy, freedom to think and form opinions without undue influence, and limiting the risks of their personal data falling into the hands of malicious actors.

Conversely, content moderation measures reflect the difficulties of providing a one-size-fits-all solution to protecting children in the digital environment. There are significant differences between a 5-year-old and a 10-year-old, a 12-year-old and a 14-year-old, and so on, not to mention that children of the same age are also individually different. While parents or caregivers may not want their toddler to watch potentially disturbing news content, it is arguably an important part of an adolescent's development that they are exposed to information about the world that may be upsetting or disturbing, such as when reading or watching the news.

The harms described in this report will vary significantly between age groups, context, individual factors such as level of maturity, and more. For example, young children may be more vulnerable than older adolescents in certain contexts and therefore need stronger protections from certain kinds of content. On the other hand, adolescents are particularly sensitive to feedback, attention and reinforcements from peers,[25] and are more risk-seeking.[26] This may require additional protections for adolescents from social media design patterns that exploit human needs for confirmation. Both the needs of children and the means to protect them change as they grow older.

Parental guidance and supervision can be an important tool to protect young children, but becomes increasingly more complicated as children grow older. For instance, it is simpler for parents or caregivers to prevent a 4-year-old from accessing digital services, than in the case of a 14-year-old. Children are also provided stronger individual rights in relation to their parents or caregivers as they grow older, for example to autonomy and privacy.[27] As it is generally more feasible, both legally and practically, to protect toddlers from online harms through individual measures such as parental supervision, this report is primarily focused on school-aged children and adolescents.

---

[24] General Data Protection Regulation (GDPR) art. 5.
[25] "Health advisory on social media use in adolescence", American Psychological Association (2023), https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use
[26] "Adolescents' heightened risk-seeking in a probabilistic gambling task", Burnett, Bault, Coricelli, Blakemore (2010). https://www.sciencedirect.com/science/article/pii/S0885201410000201
[27] General comment No. 25 para. 85.

Measures to protect and empower children and adolescents must in any case take their heterogeneity into account. This means that children of different ages may need different protective measures online, and that the measures to protect most children should not have a detrimental effect on vulnerable groups of children. It means that children and adolescents should have access to age-appropriate experiences online.[28] It is also important to give companies and regulators sufficient room for discretion to analyse and mitigate risks for more fine-grained groups of children, instead of requiring one-size-fits-all measures.

3. How are children and adolescents being harmed online?

For the past years, there have been heated debates among researchers about to what degree the use of social media leads to mental health harms among young people.[29] There is, however, ample evidence that the use of social media is linked to mental health harms, for example through feelings of exclusion, normalization of self-harm, and eating disorders.[30]

There is enough evidence to warrant action by policymakers, based on the precautionary principle. It is now widely recognised that children face several risks of harm online, which are categorised in five Cs – content, contact, conduct, contract and cross-cutting. Together, they encompass all potential risks to children's rights in the digital environment.[31]

All the major social media platforms are aggressively commercialized, designed in a way that amplifies toxic content and keep users online as often and as much as possible, and based on deeply invasive tracking and profiling of individuals. As children change and grow up quickly, the potential negative impact of each year of delayed or neglected measures cannot be overstated. As a society, we fail children if we do not take immediate actions to promote their safety and rights in the digital sphere.

While there are aspects of all digital services that may be harmful to children and adolescents, the public debate is often focused on social media platforms. This report will therefore mainly focus on various aspects of what can be called 'traditional' social media platforms such as Facebook, SnapChat, and TikTok. However, as described in section 4.2, the definition of social media is diffuse,

---

[28] "Child Rights by Design", Digital Futures Commission, 5Rights Foundation. https://childrightsbydesign.digitalfuturescommission.org.uk/
[29] "Inside the debate over The Anxious Generation", Schiffer (2024). https://www.platformer.news/anxious-generation-jonathan-haidt-debate-critique/
[30] "Social Media and Youth Mental Health", the U.S. Surgeon General (2023). https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf
[31] "The 4Cs: Classifying Online Risk to Children", Livingstone, Stoilova (2021). https://www.ssoar.info/ssoar/bitstream/handle/document/71817/ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf

and may also overlap with services such as video platforms, e-commerce, video games, etc. For the remainder of the report, the use of the term 'social media' will also, unless explicitly stated, encompass other services that facilitate interaction through digital platforms.

In the following section we describe the risks to children's rights on digital services. Measures to counter the risks are described in chapter 5, and encompass measures such as enforcing current laws, introducing targeted new provisions to fill the legal gaps in child protection, and softer measures such as governmental policies, and parental guidelines and controls.

3.1. A predatory business model

The fact that children should not be exploited commercially, does not stop companies from trying to make money off them. Researchers have found that targeting users under 18 years old generates billions in ad revenue for social media.[32] Internal Meta documents from 2021 show that Meta considers younger subgroups of children, tweens (ages 8-12), a 'valuable but untapped audience'.[33] Protecting children online therefore requires scrutiny of platforms and digital services' business models.

All the dominant social media platforms are based on a business model that rewards maximum 'engagement' – which essentially amounts to keeping users interacting with the platform. The main source of revenue for many service providers is based on selling advertising space throughout their platforms and tracking the activity of users. The service-provider promises advertisers that ads can be targeted to the right person, at the right time, which will increase the likelihood that the ad is effective. In order to do so, the service provider generally collects large amounts of data about the user, both actively provided by the user (e.g. age, gender, interests), and passively collected (e.g. inferred interests, behaviour). There are also a number of data brokers that sell personal data about individuals.

The same information is used to tailor what content is shown, as part of algorithmic recommender systems. These algorithms are tuned to maximise user interaction and the amount of time the user spends on the platform in the guise of providing personalised user experience, which gives the opportunity to show more ads. User interactions and time spent on the platform increases when users are exposed to content which elicits a strong emotional response,

[32] "Targeting kids generates billions in ad revenue for social media", Raffoul, Ward, Santoso, Kavanaugh, Austin (2024). https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0295337
[33] "Facebook's Effort to Attract Preteens Goes Beyond Instagram Kids, Documents Show", Wells, Horwitz (2021). https://www.wsj.com/articles/facebook-instagram-kids-tweens-attract-11632849667

which can lead the algorithms to favour disturbing or violent content. In short, the business model creates a vicious circle, where users are continually fed addictive and toxic content in order to be served surveillance-based advertising and leave more personal data trails, which makes the algorithms more effective.

In fact, comprehensive profiles of individual children may be used for any number of commercial purposes, and as soon such information is available from data brokers or similar actors, it is practically impossible to know who will have access or how it may be abused.[34] In the last few years, numerous technology companies have for example started trawling the entire internet for content to train artificial intelligence models. Photos from social media profiles, personal blogs, posts on internet forums, and much more is collected and used as training data. Once an AI model has been trained, it is impossible to remove any information that was part of the training data, and it is often not possible to opt out of the training.[35]

The constant collection of children's data across digital services does not only pose a threat to their right to privacy, but also to their autonomy and freedom of thought. When large amounts of behavioural and other data is collected over long stretches of time, it is possible to track most of a child's life: from the first time their parents or caregivers post a photo about them online, through the apps they use in school,[36] and when they use digital services in their free time. If these data are used to train predictive systems, it can have a has serious implications for the child's development. Prediction is by its nature based on making statistical guesses based on past observed behaviour, which means that it narrows the scope of future possibilities.

Research has shown that children are uncomfortable and feel exposed by commercial surveillance, but that they feel powerless to do anything about it.[37] This can have significant downstream 'chilling effects' on children's autonomy and freedom of speech, for example if they refrain from seeking information because they worry about how their browsing history may be used against them. As children grow and mature, they should not run the risk that their childhood behaviour and interests are used against them later in life.

---

[34] For more information about the data broker industry, see "Time to ban surveillance-based advertising", Norwegian Consumer Council (2021) https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/

[35] For a detailed overview of the harms of generative AI, see "Ghost in the machine – Addressing the consumer harms of generative AI", Norwegian Consumer Council (2023) https://www.forbrukerradet.no/side/new-report-generative-ai-threatens-consumer-rights/

[36] "'How dare they peep into my private life?' – Children's rights violations by governments that endorsed online learning during the Covid 19 Pandemic", Human Rights Watch (2022). https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[37] "'I Feel Exposed'": Caught In TikTok's Surveillance Web", Amnesty International (2023). https://www.amnesty.org/en/documents/POL40/7349/2023/en/

There is a significant power and knowledge asymmetry between large technology platforms that employ vast amounts of engineers, lawyers, designers and behavioural psychologists on one side, and children, parents and caregivers on the other. Platforms' ability to change the content and design of their services in real time, based on the child's personal data and the competences of thousands of highly qualified professionals, makes children particularly vulnerable to commercial exploitation in the digital sphere.[38]

As we describe in the following sections, the data hungry business model – which Amnesty International has deemed to be a serious threat to privacy, freedom of opinion and expression, freedom of thought, and the right to equality and non-discrimination for all users[39] – is at the core of many of the harms of social media.

3.1.1. Surveillance-based advertising and commercial pressure

Service providers such as social media platforms generally collect large amounts of data about all its users, for example location data, biometric data, identity information, and behavioural data. It has been documented that this behavioural data is used to exploit vulnerabilities by targeting advertising and other content.[40] For example, if a teenage user interacts with the platform in a way that may indicate insecurities about their physical appearance, the platform may serve content that further reinforces these insecurities and show ads for products such as weight loss drugs, dietary supplements, or cosmetic surgery.[41]

The advertising driven business model of social media platforms, alongside companies that use the platforms to advertise and sell products and services, has also led to an increasing commercialisation of almost any interaction on the platforms. From inserting advertising into news feeds, to influencers exploiting the parasocial relationships with their viewers to promote products, someone is always trying to sell you something or otherwise make a profit from you when you move around online.

For children and adolescents, the constant commercial pressure of online environments is particularly insidious. It extends to every part of children's lives, from the playroom to their bedroom and classroom. The boundaries between

---

[38] A concept BEUC calls 'digital vulnerability', see "EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy", BEUC (2022). https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf.

[39] "Surveillance Giants: How the business model of Google and Facebook threaten human rights", Amnesty International (2019). https://www.amnesty.org/en/documents/pol30/1404/2019/en/

[40] "Time to ban surveillance-based advertising", Norwegian Consumer Council (2021). https://storage02.forbrukerradet.no/media/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf

[41] "Utsettes for ny type kroppspress", Teigen, Steinnes (2019). https://www.oslomet.no/forskning/forskningsnyheter/ny-type-kroppspress.

advertising and other content are becoming increasingly blurry, making it difficult to understand if someone is trying to sell something or if they are providing entertainment or other content. Companies and influencers exploit the innate trust and naivety of young people to push products,[42] for example by mixing encouragements for content creation, games and other entertainment with advertising.[43] By launching so-called 'challenges', brands can enrol children into acting as digital advertising billboards.[44] Children might for example unwittingly promote products - including unhealthy food,[45] alcohol,[46] gambling,[47] etc. –or dangerous behaviour to other children.[48]

There are laws regulating advertising that affects children, including for digital services.[49] However, the current enforcement regimes of many of these laws are lagging behind due to the scale of illegal marketing online, are insufficient, and not dissuasive enough. Some enforcement regimes are based on self-regulatory bodies with industry representatives, with little to no real power to apply sanctions for violations.[50]

Consequently, the digital sphere may appear as a free-for-all where anyone can make a profit from targeting young people. It has also been shown that big tech companies find workarounds to target children, by creating targetable groups of an 'unknown' age, while knowing that this group consists primarily of children.[51]

---

[42] "From influence to responsibility. Time to regulate influencer marketing", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf
[43] "How children are being targeted with hidden ads on social media", Rossi, Nairn, The Conversation (2021). https://theconversation.com/how-children-are-being-targeted-with-hidden-ads-on-social-media-170502.
[44] "TikTok without filters", BEUC (2021): https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-012_tiktok_without_filters.pdf.
[45] "Food marketing to children needs rules with teeth", BEUC (2021). https://www.beuc.eu/reports/food-marketing-children-needs-rules-teeth
[46] "Picture me drinking: alcohol-related posts by Instagram influencers popular among adolescents and young adults", Hendriks, Wilmsen, Dalen, Gebhardt (2020). https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2019.02991/full
[47] "Gambling operators' use of advertising strategies on social media their effects: a systematic review", Singer, Wöhr, Otterbach (2024). https://link.springer.com/article/10.1007/s40429-024-00560-4
[48] "Under the influence of (alcohol)influencers? A qualitative study examining Belgian adolescents' evaluations of alcohol-related Instagram images from influencers", Vranken, Beullenes, Geyskens, Matthes (2021). https://www.tandfonline.com/doi/full/10.1080/17482798.2022.2157457 and "Young and exposed to unhealthy marketing", Norwegian Consumer Council (2019) https://storage02.forbrukerradet.no/media/2019/02/young-and-exposed-to-unhealthy-marketing-digital-food-marketing-using-influencers-report-february-2019.pdf.
[49] See more about these in section 5.1.
[50] See for example issues with this approach at the EU level: ("Food marketing to children needs rules with teeth", BEUC (2021), https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-084_food_marketing_to_children_needs_rules_with_teeth.pdf) and in Norway: ("Krever bedre regulering av markedsføring på nett mot unge", Norwegian Consumer Council (2020). https://www.forbrukerradet.no/siste-nytt/krever-bedre-regulering-av-markedsforing-pa-nett-mot-unge/).
[51] "Google and Meta struck secret ads deal to target teenagers", Morris, Murphy, Financial Times (2024). https://www.ft.com/content/b3bb80f4-4e01-4ce6-8358-f4f8638790f8

There is an urgent need for comprehensive action to curb illegal marketing online, to target both advertisers, the platforms selling ad space, and influencers promoting products and services to children and adolescents. This requires stronger enforcement of existing legislation concerning advertising and marketing, as well as targeted updates of the Unfair Commercial Practices Directive to implement bans on certain types of advertising to children and ensuring circumvention tactics cannot be abused by traders. These and other measures are described in sections 5.1.

3.1.2. Amplifying toxic content

Social media platforms run rampant with extreme and toxic content, such as suicide footage, violence, and substance abuse. This is a two-pronged problem, consisting of how content is pushed to users through algorithmic recommender systems, and whether content is allowed on the platform in the first place.

For adolescents and adults alike, there is an important distinction between being caught unaware by disturbing content being pushed by an algorithm, and actively seeking out such content on their own accord. Requiring companies to make changes in the way their algorithms function can in other words have an important effect on what kinds of content is recommended to individuals, and in which contexts individuals are exposed to the content.

Recommender systems

As described in the previous section, most social media platforms are funded by displaying advertising. When users are scrolling through newsfeeds or watching endless series of videos, the platform can display ads, which results in revenue. This has created a financial incentive to keep users active on the platforms as long as possible. Content that arouses anger, fear, sadness and hatred are amplified above everything else, because it generates engagement.[52] Social media companies have actively suppressed efforts to remedy this problem.[53]

The algorithmic recommender systems that control what individual users see on the platforms 'learn' by observing the user, meaning that users that interact with certain kinds of content will likely be shown more of similar – or more extreme

[52] "Facebook under fire – Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation", Merrill, Oremus, The Washington Post (2021). https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/
[53] "Facebook executives shut down efforts to make the site less divisive", Horwitz, Seetharaman, The Wall Stress Journal (2020). https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499

versions of – said content.[54] This is also known as the 'rabbit hole'-effect, where a user that originally interacted with or looked at relatively benign content is served increasingly more extreme content until they have been 'pulled down the rabbit hole', a practice that is often linked to radicalisation.[55]

There are countless examples of children and young people falling into such rabbit holes, for example with teenage girls that feel depressed being locked into content loops with increasingly more graphic and disturbing content, up to and including footage of suicide.[56] Similarly, children and adolescents in their formative years are particularly susceptible to content that exploit their insecurities, such as content about weight loss, violence, and gambling.[57]

While algorithmic recommender systems today are commonly designed to maximise attention and time spent on the platform, this is not an indispensable feature of the technology. When social media as a phenomenon started to emerge in the public consciousness, users were mainly shown content from people and organisations that they actively chose to follow.[58] This is in sharp contrast to the current social media environment, where newsfeeds, reels, and similar content recommenders mainly consist of promoted content and content that 'may be of interest to you'. End users have little control over what they are shown, because this would be less lucrative for the platforms.

Harms stemming from algorithmic recommender systems can be addressed and alleviated by strictly limiting the use of personal data for recommender systems. In addition, users must be provided more control over the content that they want to see, safer default settings, and age-appropriate design. There are already laws in place that can be used to enforce these measures, as described further in sections 5.1.

---

[54] See for example "Recommender systems and the amplification of extremist content", Whittaker, Looney, Reed, Votta (2021) https://policyreview.info/articles/analysis/recommender-systems-and-amplification-extremist-content, "Fixing recommender systems", Panoptykon, Irish Council for Civil Liberties, People vs. Big Tech (2023). https://panoptykon.org/sites/default/files/2023-08/Panoptykon_ICCL_PvsBT_Fixing-recommender-systems_Aug%202023.pdf, and "When my dad was sick, I started Googling grief. Then I couldn't escape it", Ryan-Mosley (2023). https://www.technologyreview.com/2023/02/06/1067794/escape-grief-content-unsubscribe-facebook-instagram-amazon-recommendation-algorithms/.

[55] "YouTube Regrets: A crowdsourced investigation into YouTube's recommendation algorithm", Mozilla (2021). https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf

[56] "Driven Into Darkness: How TikTok encourages self-harm and suicidal ideation", Amnesty International (2023). https://www.amnesty.org/en/latest/news/2023/11/tiktok-risks-pushing-children-towards-harmful-content/

[57] "Pathways: How digital design puts children at risk", 5Rights Foundation (2021). https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf

[58] "Social Quitting", Doctorow (2023). https://pluralistic.net/2023/01/08/watch-the-surpluses/

Content moderation

The existence of toxic content must also be dealt with by content moderation on the platforms. However, content moderation is very difficult to do well – it is essentially an attempt at a technological solution to a series of complex problems.[59]

Under-moderation means that toxic content proliferates. Meanwhile, over-moderation can limit important rights such as freedom of expression and access to information. This is especially true with automated content moderation, where the effectiveness of content moderation may be measured based on scale and quantity, rather than accuracy.

Some content, such as TikTok videos idealising and romanticising self-harm, may seem to be obviously harmful and not something to be watched by anyone, let alone minors. However, even in such cases it can be exceedingly difficult to draw distinctions between whether a certain type of content is actively harmful or not, as context matters – spreading awareness about mental illness is not the same as promoting self-harm. Similarly, there is no clear-cut legal definition of the concept of 'harmful content'.[60]

The designation of harmful content is highly cultural and political. In some parts of the world, learning about topics such as sexuality or gender expression is seen as controversial and unsuitable for minors, while in some countries this is part of educational programmes and considered to be vital for particularly vulnerable groups.

On a political level, there are ongoing debates about whether imagery displaying war crimes and other atrocities should be allowed on social media platforms.[61] While such imagery is undoubtably disturbing, it is often also a crucial way to spread awareness. While it may seem clear that an 8-year-old should not be exposed to such content, it is questionable whether a 14-year-old needs the same level of protection.

Furthermore, aggressive content moderation without sufficient transparency and effective complaint mechanisms inevitably lead to situations where legitimate content is taken down or accounts are banned with insufficient explanations and complaint mechanisms. Opaque moderation practices also

---

[59] "Treating the symptoms or the disease? Analysing the UK Online Safety Act's Approach to digital regulation", Nash, Felton (2024). https://onlinelibrary.wiley.com/doi/pdf/10.1002/poi3.404
[60] "The perils of legally defining disinformation", Fathaig, Helberger, Appelman (2021). https://policyreview.info/articles/analysis/perils-legally-defining-disinformation
[61] "Meta's Broken Promises: Systematic Censorship of Palestine Content on Instagram and Facebook", Human Rights Watch (2023). https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

diminish the ability of researchers to assess the effectiveness of content moderation.

The harms stemming from toxic content can be alleviated by curbing the dissemination and reinforcement of illegal and toxic content through recommender systems, as outlined above. It is important to distinguish between measures that prevent users from being able to access content at all, and that prevent the platform from actively pushing the content. This must be complemented by stronger, more robust, human-controlled and transparent content moderation practices by platform providers, content warnings, and the implementation of age-appropriate design features, as described further in sections 5.2 and 5.3

3.1.3. Addictive mechanisms and excessive screentime

One of the major concerns of internet usage amongst young people is excessive screentime. It is widely reported that smartphone usage may come in the way of most other aspects of children's lives, such as school, physical activities, sleep, and physical eye damage.[62] While this is arguably also a problem facing many adults, the impact of screentime on children and adolescents is particularly problematic if it affects other crucial aspects of their lives while they are still growing up, such as physical activities and wellbeing, free play, the development of social skills, education, etc.

As described in the previous sections, the business model of social media platforms has created a strong incentive to keep users hooked (or 'engaged') for as long as possible, by any means. The algorithmic content recommender systems continuously optimise for engagement, which creates an addictive dopamine-triggering feedback loop where users are constantly bombarded with content that the algorithm has calculated will keep the user scrolling, clicking, or watching.[63]

Platforms also nudge content creators to create content that will keep users scrolling, clicking or watching, for example by funding creators who post content which leads to engagement.[64] The most successful content creators are experts at exploiting these algorithms, tailoring their content to maximise views and

[62] "Digital Screen Use and Dry Eye: A Review" Mehra, Galor (2020). https://www.sciencedirect.com/science/article/pii/S216209892300155X
[63] "What Makes TikTok so Addictive?: An Analysis of the Mechanisms Underlying the World's Latest Social Media Craze", Petrillo (2021). https://sites.brown.edu/publichealthjournal/2021/12/13/tiktok/
[64] "Facebook Content Monetization Beta", Meta. https://creators.facebook.com/programs/bonuses/?locale=en_US

dissemination.[65] This can for example amount to massive amounts of AI-generated pictures being used to churn out content at a rapid rate.[66]

In order to make sure that users keep returning to the platforms, service providers often use mechanisms such as notifications or 'streaks'. Other design tricks are then employed and continually refined to keep the user glued to the screen. For example, many video-sharing platforms use auto-play functionality, where the user is always shown a new video without having to actively ask for it. Such addictive mechanisms are deliberately designed to foster addictive behaviour in users.[67]

With the introduction of generative AI services, companies can automate and customise interactions with individual users. Chatbots marketed as virtual friends open new avenues for parasocial relationships, while simulated emotion and 24 hour a day availability lay the groundwork for potential addiction and manipulation.[68] It is particularly problematic that such AI features are rolled out and pushed at children and adolescents, who may have difficulties understanding that the AI system is not a person and does not feel emotions.

With concerns about screentime on the rise, many technology companies have started to introduce features to "reduce screentime". These features require critical scrutiny. For example, TikTok's internal documents show that their time-limit tools have very limited impact on screentime, and are primarily introduced as policy talking points and to improve public trust.[69] Instead of actually changing the addictive mechanisms, platforms can in this way introduce ineffective features, which gives a deceptive impression of accountability.

Addictive mechanisms can be curbed by strong and ambitious enforcement of existing laws, and by introducing new legal requirements to reduce the use of addictive mechanisms and deceptive design patterns. Service-providers should be obligated to design their platforms to be fair and safe, and should also provide functional parental controls with age appropriate default settings for screen time. Additionally, governments should publish fact-based, clear, and easy to

---

[65] "Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram", Cotter (2019). https://pure.psu.edu/en/publications/playing-the-visibility-game-how-digital-influencers-and-algorithm

[66] "Where Facebook's AI Slop Comes From", Koebler, 404Media (2024). https://www.404media.co/where-facebooks-ai-slop-comes-from/

[67] "EU lawmaker points to mental health risks for online services' addictive design", Tar, Euractiv (2023). https://www.euractiv.com/section/platforms/news/eu-lawmaker-points-to-mental-health-risks-for-online-services-addictive-design/

[68] "One is the loneliest number... Two can be as bad as one. The influence of AI Friendship Apps on users' well-being and addiction", Marriott, Pitardi (2023). https://onlinelibrary.wiley.com/doi/10.1002/mar.21899

[69] "TikTok executives know about app's effect on teens, lawsuit documents allege", Allyn, Goodman, Kerr, NPR.(2024). https://www.npr.org/2024/10/11/g-s1-27676/tiktok-redacted-documents-in-teen-safety-lawsuit-revealed

follow guidelines to help parents and caregivers set time limits for their children's screen use. These measures are described further in section 5.

3.2. Other major issues

So far, this report has outlined a number of risks that children face online. Not all harms from digital services can or should be understood through the consumer lens.

Therefore, we briefly outline some of the most widely discussed harms from digital services in the following, notably mental health harms, cyberbullying and unwanted interactions with strangers. These issues can also be intertwined with the business model described above.

3.2.1. Mental health harms

The past years have involved a drastic negative development when it comes to youth's mental health. Leaks from Facebook have shown that the company knew that its platform had a negative effect on teenagers and children,[70] and the US general surgeon published an alarming report in 2023 about social media and children's mental health and well-being.[71]

Social media use may affect users' self-perception in various negative ways, which children and adolescents are especially vulnerable to. Features such as 'likes' are for example a seemingly clear and quantifiable measure of social approval or disapproval. This preys on the need for affirmation and the fear of missing out, and may create or exacerbate existing insecurities, leading to stress, depression, and other mental health issues.[72]

There is an onset of influencers and other commercial actors who publish content that can have a negative effect on children and adolescents' self-perception. This can come in the form of self-improvement videos, pornographic material,[73] problematic dieting and exercise programmes disguised as well-being programmes, or advertising for cosmetic surgery and

---

[70] "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show", Wells, Horwitz, Seetharaman, The Wall Street Journal (2021). https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[71] "Surgeon General Issues New Advisory About Effects Social Media Use Has on Youth Mental Health", U.S. Department of Health and Human Services (2024). https://www.hhs.gov/about/news/2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html

[72] "Fear of missing out and social networking sites use and abuse: A meta-analysis", Giulia Fioravanti, Silvia Casale, Sara Bocci Benucci, Alfonso Prostamo, Andrea Falone, Valdo Ricca, Francesco Rotella, Computers in Human Behavior, Volume 122 (2021). https://doi.org/10.1016/j.chb.2021.106839

[73] "Undress or fail: Instagram's algorithm strong-arms users into showing skin", Algorithm Watch, European Data Journalism Network (2020). https://algorithmwatch.org/en/instagram-algorithm-nudity/

anti-aging products[74], alcohol, gambling, risky financial products etc. Recommender systems can also be finetuned to prioritise content about people considered beautiful, and apps can provide beauty filters, both of which can in turn affect body image.[75]

While issues related to children's mental health and wellbeing cannot be solely seen through the lens of digitalisation and social media, there are important measures that can help reduce the mental strain of children if implemented in the digital sphere. Many of the issues are exacerbated by the aggressive commercialisation, amplification of toxic content and addictive mechanisms already mentioned in this report.

There should therefore be stronger regulation on advertising, including bans on certain types of advertising to children and adolescents, as described in sections 5.1.1 and 5.1.2. Furthermore, enforcement of rules that reduce or remove addictive mechanisms, design that leads to the proliferation of toxic content, and other intrusive profiling practices, can also be important tools to combat mental health harms online.

3.2.2. Cyberbullying

While social pressure and bullying are not exclusive to online spaces, the proliferation of social media has turbocharged negative interactions. These interactions can have strong negative effects both when they happen with people within the child or adolescent's social circles, and in unsolicited interactions with strangers.

Social media platforms create new challenges related to social exclusion and other forms of bullying. Constant status updates from friends create an impression that everyone else lives a better and more fulfilling life, are more popular, and so on. Apps send push notifications throughout the day to 'remind' users that everyone else is always enjoying themselves. Location sharing features such as SnapMap may make children and adolescents feel left out by showing other people attending the same party, going to a concert together, etc.

[74] "Young girls are using anti-aging products they see on social media. The harm is more than skin deep", Gecker, The Associated Press (2024). https://apnews.com/article/influenced-skincare-routine-mental-health-f59bb09114ab93323e3a47197a1ad914

[75] "TikTok executives know about app's effect on teens, lawsuit documents allege", Allyn, Goodman, Kerr, NPR (2024). https://www.npr.org/2024/10/11/g-s1-27676/tiktok-redacted-documents-in-teen-safety-lawsuit-revealed

In other cases, anonymous messaging apps[76] and disappearing message features[77] have been used by children to harass and bully other children.

The focus on sharing user-generated content can also have particularly damaging effects on young people. Even if content such as pictures is first voluntarily shared, they may quickly be disseminated beyond the child's control. The problem can be further compounded if parents, caregiver or someone else unwittingly share photos of the child. The nature of the internet means that having content removed once it has been spread is practically impossible, which can lead to extreme turmoil for the person whose content is shared. Negative effects can therefore persist in perpetuity or resurface over time and in new contexts.

Cyberbullying, including unwanted sharing of photos, are part of a broader social issue, although the internet has turbocharged the phenomenon. The problems of cyberbullying consequently cannot be wholly addressed through technical or legislative means, but must be part of education and training for young people to become digital citizens, in addition to other types of interventions.[78]

Cyberbullying is an alarming issue, but is outside the Norwegian Consumer Council's mandate, and therefore this report. None the less, certain design elements that may facilitate cyberbullying, such as likes, self-destructing content and disappearing messages features can be removed by platforms to reduce the harm. Some of these are closely connected to the platforms' business models. Recommendations on how to make the digital sphere empowering for children are described in chapter 5.

3.2.3. Unwanted interactions with strangers

Unwanted interactions with strangers are also a major concern when children use social media platforms, which can for example lead to online sexual exploitation of children.[79] It is possible to reduce this issue by introducing features such as not allowing messages from strangers to profiles belonging to children and adolescents, and disabling the possibility for children's accounts to be recommended to strangers.[80] While interactions with strangers are a serious

[76] "Millions of teens are using a new app to post anonymous thoughts, and most parents have no idea", Balingit (2015). https://www.washingtonpost.com/local/education/millions-of-teens-are-using-a-new-app-to-post-anonymous-thoughts-and-most-parents-have-no-idea/2015/12/08/1532a98c-9907-11e5-8917-653b65c809eb_story.html
[77] "Gone in a Flash: How Disappearing Messages Can Impact Your Child's Online Safety", Mobicip (2024). https://www.mobicip.com/blog/gone-flash-how-disappearing-messages-can-impact-your-childs-online-safety
[78] "Ending the torment: tackling bullying from the schoolyard to cyberspace", UNICEF (2016). https://www.unicef.org/media/66536/file/Ending-the-torment.pdf
[79] "Child Sexual Exploitation", EUROPOL. https://www.europol.europa.eu/crime-areas/child-sexual-exploitation
[80] "Risky-by-Design. Case study: Friend suggestions", 5Rights Foundation. https://www.riskyby.design/friend-suggestions

issue, they are outside the Norwegian Consumer's mandate, and therefore outside the scope of this report.

There are various helplines accessible to children and their parents and caregivers, in cases of cyberbullying, unwanted interactions with strangers, or other cases of problematic situations. These will generally vary between countries.[81]

4. Technically blocking children and adolescents from digital services is a more complicated measure than it seems

In public debates, removing children from services is considered one of the most important ways to protect children from the harms outlined above. This measure resurfaces in various settings, such as in policy debates[82] and in decisions from enforcement authorities.[83]

While the negative effects of social media should not be understated, there are significant risks associated with completely shutting them out, especially adolescents. This may exclude them from services or activities in a way that limits their ability to enjoy all their rights online, as outlined in chapter 2.

Strict, technical measures to ban children and adolescents under a certain age from digital spaces, can also introduce new problems and risks. Many of these risks apply not only to children and adolescents, but to all adults as well. For example, any requirements to provide identification papers on social media platforms will inevitably require all adults to identify themselves as well.

As we will describe in the following sections, measures that target certain platforms (such as TikTok, Snapchat or Instagram) will necessarily leave major blind spots. There are also serious concerns that initiatives to block young people from social media are simply ineffective to protect children online and may even make matters worse. An important backdrop is that several reports

[81] For Norway, this is available here: "Barn, ungdom og voksne – her kan du snakke, chatte og få hjelp", Redd Barna. https://www.reddbarna.no/her-kan-du-fa-hjelp/
[82] EU discussion ("European authorities press on with digital wallets for social media age verification", Gkritsi, Euractiv (2024). https://www.euractiv.com/section/tech/news/european-authorities-press-on-with-digital-wallets-for-social-media-age-verification/) and the Norwegian discussion ("Støre vil ha aldersgrense for sosiale medier", Jobling, NRK (2024). https://www.nrk.no/norge/store-vil-ha-aldersgrense-for-sosiale-medier-1.16944311).
[83] "Vulnerable Individuals. Tools for Online Protection. Children and Age Verification – Spring Conference 2023", Garante per la Protezione dei Dati Personali (2023). https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9965235

have concluded that none of the technical measures that exist today to block children from digital services satisfy the requirements to be rights-respecting.[84]

4.1. Should children and young people be excluded from social media?

When considering whether to introduce strict technical barriers to social media platforms, policymakers should also take children's legitimate reasons to be online into account. This is especially important because there exist other, effective measures that can be introduced to reduce the harms children face online, which do not impose limitations on children's other rights.

There are very legitimate reasons why children over a certain age need access to many of the platforms that policy makers currently consider age gating. For example, many children and adolescents - especially from their early teens – use social media to participate in civic life, keep up to date on current events, and to mobilise around causes they care about and that affect them. This may be anything from local youth groups and activities to global campaigns such as Fridays for Future.[85]

Social media platforms have been important mobilisation tools for grassroots campaigns all over the world, which is one of the few ways children can make their voice heard. If adolescents are removed from access to social media platforms or similar digital services, these voices may be silenced in online spaces.

As civil and political discourse are increasingly moving into digital spaces, an effective shutout from these spaces may deprive young people of significant parts of their civic education. A presence in online spaces may let young people learn about the world, be exposed to different cultures, opinions and opportunities, and help them develop critical thinking skills, decision-making and autonomy.

While social media platforms can clearly sow division, they also bring people together, and can be a lifeline for many young people. For example, online communities can allow children and adolescents who feel alone make contact with like-minded people – making them feel less alone. This can be particularly important for children who belong to LGBTQ+ communities, but who may feel

[84] See e.g. "Trustworthy Age Assurance?", Sas, Mühlberg, Greens/EFA (2024) https://extranet.greens-efa.eu/public/media/file/1/8760 and "Online age verification: balancing privacy and the protection of minors", CNIL (2022). https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.
[85] "Gen Z: How young people are changing activism", Carnegie, BBC (2022). https://www.bbc.com/worklife/article/20220803-gen-z-how-young-people-are-changing-activism

isolated if they are growing up in a small town. Children and adolescents with disabilities may also use digital services to connect and interact with other children, such as through online video games.[86]

4.2. Defining social media is a complicated endeavour

Public debates are often focused on social media as a particular type of digital service that creates harms to children and young people. However, there is no broad consensus on what exactly constitutes a 'social media platform'. While major services such as Facebook, Instagram and TikTok clearly fall within the scope of 'social media', the lines become increasingly blurry when trying to delineate the defining features of a social media platform. This has implications for the intrusiveness of mandatory technical bans of children under a certain age.

Social networking is often a key or ancillary component of services that would perhaps not typically be thought of as social media platforms. For example, this may include services such as messaging apps (iMessage, WhatsApp, Signal), video games (Roblox, Fortnite), message boards (Reddit, Discord), and practically any service that includes comment sections and similar features, such as video platforms (YouTube) and news websites.

Wikipedia defines social media as 'interactive technologies that facilitate the creation, sharing and aggregation of content, ideas, interests, and other forms of expression through virtual communities and networks'.[87] This usually includes features such as social networking, user-generated content, algorithmic feeds, and user-curated profiles.

The European Digital Services Act also includes a reference to social media, stating that 'Online platforms, such as social networks [...], should be defined as providers of hosting services that not only store information provided by the recipients of the service at their request, but that also disseminate that information to the public at the request of the recipients of the service.'[88] In practice, disseminating information to the public means that information should be available to an unlimited number of persons.[89] While this definition appears to exclude messaging apps, it may include any types of message boards.

When contemplating how to protect children and adolescents from the harms of social media, it is necessary to have a clear view of what kind of platforms that

---

[86] "Først da Mats var død, forsto foreldrene verdien av gamingen hans", Schaubert, NRK (2019). https://www.nrk.no/dokumentar/xl/forst-da-mats-var-dod_-forsto-foreldrene-verdien-av-gamingen-hans-1.14197198
[87] "Social media", Wikipedia. https://en.wikipedia.org/wiki/Social_media
[88] DSA rec. 13.
[89] DSA rec. 14.

should be targeted with preventive measures, and which types of preventive measures are necessary and relevant. Many of the harmful effects described above are not isolated to the 'traditional' social media platforms and may be just as prevalent in other types of services such as educational platforms, e-commerce services, and video games. With a narrow definition of social media, the harms that children and adolescents must be protected from may continue on platforms and services that are not covered.

4.3. Excluding children under a certain age does not protect children over the age limit

As described in chapter 3, many digital platforms are characterised by a predatory business model, which results in aggressive commercial practices, extensive privacy violations, the amplification of toxic content, and addictive mechanisms. Measures to exclude children under a certain age from social media platforms do not address how platforms engage in any of these harmful practices. This means that anyone over the age limit, including individuals who are still legally considered children because they are under 18 years of age, will continue to be exposed to deeply problematic and harmful business practices.

Introducing a hard, technical age gate – meaning that anyone who doesn't satisfy the verification requirements are shut out – to even the most popular digital services will be both time-consuming and costly. It is also likely to come at the expense of other initiatives, such as targeted measures to prevent harms that arise on the platforms due their design. This means that companies will continue to expose children that are over an age limit (for example 13 or 15) to toxic content such as senseless violence and promotions of eating disorders and suicide. Similarly, the addictive designs on the platforms will continue unabated, and companies may continue to exploit children's vulnerabilities to target content and advertising to them.

Furthermore, by focusing efforts on introducing hard age gating to digital services, the market for age assurance solutions may grow, at the expense of age-appropriate digital services that focus on design for children's security and wellbeing. There are many ways that digital services can be used to empower children, if they are designed in a rights-respecting manner. This could for example be an app which can be used to coordinate social activities among 10- to 12-year-olds, or to allow young people to have their voices heard on political issues that concern them. In general, children should be protected through empowerment, not exclusion.

4.4. Technical solutions are risky and not fool-proof

If it is deemed necessary to ensure children and adolescents under a certain age do not get access to a platform, one must address the question of how to practically impose such an age limit. This requires that digital service providers know whether a user is a child or not.

The umbrella term for methods to gauge a user's age is 'age assurance', which encompasses methods to find out the exact age of an individual ('age verification'), and methods to infer the approximate age or age range of an individual ('age estimation').

While age assurance technologies may be intended to prevent children from accessing certain services, they inevitably require *everyone* to verify their age. This includes university students, people with disabilities, immigrants, seniors, and other teenagers and adults over the age limit. Age assurance technology thus adds an additional barrier between every person in society and what could be important digital services, which makes such technology more intrusive than it appears at first glance. Different groups in society also have different prerequisites to using digital services, access to identity papers, and more.

The timing and frequency of age assurance is also important. Age assurance can for example be employed the first time someone accesses a service, when someone creates a profile or account, or every time someone accesses a service. The more often age assurance is employed, the more difficult it might be to circumvent the measure over time. At the same time, frequent age assurance checks exacerbate the risks associated with the age assurance method in use.

The most widely discussed age assurance method at the EU level and in a Norwegian context is age verification based on different forms of electronic ID solutions.[90] At the EU-level, the introduction of age verification technology is expected to be based on the upcoming European eIDAS regulation, which provides a list of requirements for a technical digital identity framework.[91] As ID-based age verification is the most politically and regulatory salient issue, we therefore commit substantial space in the report to the risks of this particular solution.

---

[90] See for example "Støre vil ha aldersgrense for sosiale medier", Jobling, NRK (2024) https://www.nrk.no/norge/store-vil-ha-aldersgrense-for-sosiale-medier-1.16944311, "Unreleased document: DSA, identity wallets take spotlight on protection of minors online", Gkritsi, Euractiv (2024). https://www.euractiv.com/section/digital/news/unreleased-document-dsa-identity-wallets-take-spotlight-on-protection-of-minors-online/

[91] "eIDAS Regulation", European Commission. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

4.4.1. ID-based age verification

ID-based age verification relies on some kind of official proof-of-age. Such official documents are also often a proof of identity, such as passports, national ID cards, or a digital electronic identification based on national identity documents (eID).

There are several reasons why ID-based age verification can be particularly risky for children and for consumers in general. The main risks can be categorised as digital and societal exclusion, privacy and data protection, and security.

Exclusion

ID-based verification means that *everyone, regardless of age,* will have to identify themselves, and consequently involves significant risks of exclusion. Regardless of what kind of technological measure that is implemented, individuals need to have access to relevant proof of identity to access social media services, and whichever other services that implement age verification. People who do not have access to the required proof of identity will not be able to access the services.

There are various reasons why people do not have access to proof of identity. This also varies depending on the country. For example, although Norway is by all measures a highly digitised country, around 400 000 (or 7 % of the population), do not have access to or use an electronic ID.[92] If electronic ID becomes a requirement to access various digital services, these consumers will effectively be excluded from these services.

Since social media platforms are now an essential part of everyday life, exclusion may have significant negative consequences for many consumers who are already marginalised. For example, senior citizens may be cut off from communicating with their families, or immigrants may be excluded from platforms that would otherwise provide contact with new neighbours or potential employers.

Privacy and anonymity online

There are many perfectly legitimate reasons to want to remain anonymous online. On a basic level, people may wish to avoid being tracked and profiled for commercial purposes. For example, someone who is nervous about a possible medical issue may not want their search history about the issue to be used for advertising or for this information to be sold to third parties.

---

[92] "Outsiderness in the consumer markets", Norwegian Consumer Council (2023) p. 10. https://storage02.forbrukerradet.no/media/2023/01/forbrukerradet--outsiderness-in-the-consumer-markets-en.pdf

Anonymity online is particularly important to protect vulnerable groups or individuals. Political dissidents or activists that fear being targeted for their beliefs is one such example. Human rights activists organising to expose and/or protest against repressive practices may be dependent on anonymity to avoid harassment or dangerous repercussions. Similarly, after the right to abortion was repealed across many states in the US, reports emerged of women being prosecuted due to crossing state lines to access reproductive health services.[93] Without anonymity, these women had no way to stay safe when seeking help.

If mandatory ID-based age verification schemes are imposed on digital platforms, the possibility to remain anonymous may be severely diminished. As outlined below, there are tools for circumvention that can be used to bypass such measures, but for vulnerable groups without the knowhow or capabilities to do so, the lack of anonymity can become dangerous. Even if one doubts that identity verification would be abused in a Norwegian setting, the signalling effect to other, repressive regimes, should not be underestimated.

The introduction of ID-based age verification must be understood in the context of today's prominent business model of advertising based on surveillance. Connecting real world identities to online profiles is a golden opportunity for companies engaged in tracking and profiling consumers for commercial purposes. Cross-device and cross-service tracking is extremely attractive to these companies, because it allows them to create even more detailed and granular profiles of individual consumers. An ID-based age verification scheme that 'guarantees' that different user profiles on different services belong to the same individual, is a powerful persistent identifier that can be used to further undermine consumer privacy.

Although the General Data Protection Regulation (GDPR) came into force in the EU in 2016, countless companies have kept consistently breaking the law because surveillance is extremely profitable – for example for the purpose of advertising, but also to train data-hungry AI models. Unless it is technically impossible to connect the information about *who* is accessing a service, to *which kind of service or content* they access (dubbed a 'zero-knowledge proof' or a 'double-blind'), it should be expected that companies will try to circumvent any technical, legal or organisational barriers. This would leave both adults and children even more vulnerable to invasive tracking practices than they are today.

An ID-based age verification solution which involves a 'double blind' and therefore does not track individuals, can still be problematic in a privacy perspective. When individuals feel like they are being watched, they often

[93] "Location Data Tracks Abortion Clinic Visits. Here's What to Know", https://www.eff.org/deeplinks/2024/03/location-data-tracks-abortion-clinic-visits-heres-what-knowHere's What to Know", Electronic Frontier Foundation (2024).

change their behaviour accordingly (called a 'chilling effect'). This can for example translate to not searching for topics and services perceived as sensitive, such as information about sexual orientation or helplines for bullying. The chilling effect does not necessitate that someone is truly watching what you are doing, simply that it feels like they are. An ID-based age verification solution runs the risk of giving this impression, regardless of whether information about the individuals is stored and repurposed.

Any mandatory verification mechanisms must be implemented in accordance with the strict requirements set forth in the GDPR. It is not acceptable that verification mechanisms are used for any purposes other than determining the age of the subject. Use of the verification system must not be logged or otherwise registered beyond what is needed to verify the subject's age. In addition, age verification must not be mandated if it can have a chilling effect, especially regarding information, bulletin boards, or networks that relate to topics that can feel sensitive for children.

Security risks

If service-providers are compelled or otherwise incentivised to verify their users' age and/or identity, this will probably involve more collection of personal data. Verification can lead to the centralisation of valuable information, and may increase the attractiveness of black-market access to credentials.[94] When such troves of information are collected and stored, the companies that hold the information may become attractive targets for malicious actors.

If a database containing large amounts of personal data is hacked or otherwise breached, this can have many harmful consequences, including identity theft, blackmail, ransomware and fraud. Measures such as scanning and uploading passports, or biometric identification schemes are particularly concerning. If such information ends up in the wrong hands the damage may be irreversible. The risks of this may increase with the number of age verification providers on the market, who may have different approaches to cybersecurity.

There is already a plethora of examples of security breaches. In 2024 a third-party provider of ID-based age verification for services such as TikTok and X was revealed to be compromised, exposing the driver licenses of end users that had verified their identities.[95] Similarly, the US-based telecommunications company

[94] "Age against the machine: the race to make online spaces age-appropriate", EDRi (2024). https://edri.org/our-work/age-against-the-machine-the-race-to-make-online-spaces-age-appropriate/

[95] "ID Verification Service for TikTok, Uber, X Exposed Driver Licenses", Cox, 404Media (2024). https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/

AT&T was hacked in 2024, compromising complete datasets of call and text records of consumers.[96]

It is key that governments require sufficiently strong security measures through regulations and standards. The recently published technical reference document for an EU-wide eID solution[97] has been criticised by a broad group of civil society organisations and researchers for only requiring old-fashioned cryptography mechanisms.[98]

Ease of circumvention

Even if ID-based age verification is mandated for certain digital services and platforms, there is a significant risk that young people will be able to circumvent any hard technical barriers, rendering them ineffective. This can happen through switching to alternative services, or by finding ways to bypass the age verification measure to access the platform in question.

Switching to alternative services

Although the major social media platforms are dominant actors online, they are not the only available service providers. Young people that are shut out of the largest platforms could quite easily move to smaller alternative platforms that have not implemented verification measures.[99]

There are high barriers for adults to move away from large online platforms, due to network effects. Simply put, if your relatives, your friends from school, your coworkers and your children's leisure activities are all connected on Facebook, it is not realistic for you to move to a different platform. The switching cost is simply too high. For children and adolescents, the switching cost is lower, since younger people have fewer social connections in general, and may be more curious about new services. This can be observed by how new apps and services keep appearing and enjoying rapid surges in popularity in a short amount of time, as younger users move to the 'new thing'. For example, the messaging app BeReal gained rapid popularity in 2022, and quickly became one of the most downloaded apps in the world. In less than a year, the user base dwindled as other services took its place.[100]

---

[96] "The Sweeping Danger of the AT&T Phone Records Breach", Newman, WIRED (2024). https://www.wired.com/story/att-phone-records-breach-110-million/
[97] As required by the eIDAS regulation.
[98] "Euopean eID Implementation, Open Letter", epicenter.works et al. (2024). https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_-_European_eID_Implementation_Open_Letter.pdf
[99] "A booming industry of AI age scanners, aimed at children's faces", Harwell, The Washington Post (2024). https://www.washingtonpost.com/technology/2024/08/07/face-scanning-kids-online-privacy/
[100] "They're Over Being Real", Holtermann, The New York Times (2023). https://www.nytimes.com/2023/04/13/style/bereal-app.html

If major platforms are made to implement age verification, this may succeed in keeping a lot of younger users off those particular platforms. This does not stop the same users from moving to a different platform that has not implemented age verification. In other words, if the major social media platforms start blocking out younger users, young people can very easily simply move to a smaller alternative where they are not shut out.

If younger users start moving to alternative platforms without age verification, this can generate new or exacerbate existing harmful effects. For all their faults, most of the largest platforms have at least some types of content moderation practices and security measures in place, if only because they face scrutiny from regulators or the public. Smaller actors will have less money to spend on mitigating measures, may face less scrutiny, and in many cases lack an incentive to invest in security, privacy, safety and content moderation. This means that technical measures to shut young people out may push them toward services that are even worse than the current dominant platforms.

The only way to prevent children and adolescents from moving to alternative platforms and services, is to age-gate the entire internet. This would require policymakers and regulators to somehow ensure that services that do not abide by strict age verification rules are not accessible to children through other measures. In theory, this could amount to requiring internet service providers (ISPs) to block access to certain services on the network layer. Since we have already established that defining social media is difficult, lawmakers would have to give regulators the mandate to block or shut down a broad set of services.

In such a scenario, regulators would also need the powers to act expediently to catch and block new service providers as they enter the market. Such speedy action is unlikely, given the timespans of other regulatory action in the digital sphere, where regulatory action can take many years – which amounts to a large part of children's lives. The alternative is for ISPs to only allow pre-approved web pages and apps to be accessible in Norway or the EU. This amounts to a national firewall, which would amount to broad censorship of the internet, and which is unacceptable in democratic societies.

Any mandatory verification mechanisms must not involve ISP-level filtering of the internet or similarly invasive anti-circumvention measures. Such measures would amount to complete censorship of the internet.

Technical circumvention

National or regional blocks or restrictions on certain services or platforms can be circumvented through technical measures. Tools such as virtual private networks (VPNs) allow users to route their internet traffic through a third party, making it appear as though the user is situated in a different location – such as a

country that does not block social media platforms for minors. Age verification systems that are implemented on a national or regional level, or anything else than world-wide coverage, can thus easily be bypassed through installing ancillary software tools, something many adolescents are already proficient at.

If children access these services through a VPN routed from outside the EU (or similar technologies), they will also be afforded lower protections. For example, the US does not have a federal data protection law – leaving children accessing TikTok or Instagram from the US with weaker levels of data protection than European adults.

Children and adolescents can also find other ways to circumvent age verification, by fooling the technical implementation. They can for example use fake IDs, borrow IDs from friends or family, and buy selfie videos or pictures if the age verification provider requires additional proof.[101] Once children find methods to circumvent age verification, the methods can spread quickly among peers.

Malicious actors may circumvent age verification tools for the opposite purpose: to gain access to, and therefore trust within closed spaces. They can pretend to be children by using fake IDs, and enter supposedly safe spaces unhindered by taking advantage of the false sense of security age verification systems can create.

In practice, it is next to impossible to create a fool-proof age verification system; it is a purely technical fix to a combination of many complex technical and social issues experienced by children online. If the solution is only focused on keeping children away from the service, they will attempt to bypass the system. Age verification providers will have to increase the control and surveillance measures, to counter new methods for circumvention as they develop and spread among children and adolescents.

4.4.2. Risky age estimation techniques

In addition to the aforementioned ID-based age verification techniques, there are several notable age assurance techniques based on age estimation. These carry many of the same risks as ID-based solutions, in addition to some risks that are specific to such techniques.

It is worth keeping in mind that age estimation is inherently problematic if used to determine whether individuals should be allowed to access services, because age limits are binary – either you are old enough to access the service, or you are

[101] "A booming industry of AI age scanners, aimed at children's faces", Harwell, The Washington Post (2024). https://www.washingtonpost.com/technology/2024/08/07/face-scanning-kids-online-privacy/

shut out. If age estimation is used to determine access, access to services will essentially be arbitrary based on an educated guess. The alternative is to combine age estimation with age verification, whenever someone is flagged by the age estimation system. That would introduce all the risks from age verification systems, as described previously in this report.

Profiling users

It is possible to estimate users' age through profiling, which entails collecting and analysing personal data about individuals' behaviour. This solution may seem tempting, because many digital service providers already profile their users extensively for commercial purposes. However, repurposing such data points to uncover whether there are children on a service is very problematic.

As described in section 3.1, the current business model of personal data collection and reuse allows companies to infer children's vulnerabilities, while also fuelling the design and proliferation of addictive mechanisms, the amplification of toxic content, and training AI models. By requiring companies to profile users to estimate their age, policymakers would in practice legitimise deeply invasive surveillance practices, which have been widely criticised by civil society.[102]

Profiling practices as a basis for age assurance also increases the risk of digital exclusion for anyone with behaviour outside the range of 'normal', such as individuals with intellectual or developmental disabilities,[103] which may lead to being incorrectly flagged as underage.

Biometrics

Age verification can be based on the use of biometrics to estimate an individual's age. This can for example be facial analysis of an uploaded picture or a video.

Biometric data is extremely sensitive information. It is not possible to change one's biometric features on demand, and if biometric data is leaked or subject to a data breach, the risks of misuse are profound. If the online behaviour of individuals is connected to a trait that cannot be changed, this is also a serious violation of privacy and data protection.

Biometric facial analysis systems are also notoriously inaccurate and error prone. Such systems can struggle to verify the age of children or adults who are

[102] "International coalition calls for action against surveillance-based advertising", Norwegian Consumer Council (2021). https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/
[103] "Invisible No More: The Impact of Facial Recognition On People with Disabilities", eticas. https://eticas.ai/invisible-no-more-the-impact-of-facial-recognition-on-people-with-disabilities-2/

close to the age limit, because the algorithms' accuracy typically range between 2-4 years at best.[104] This means that some children who should get access, will be locked out of the platforms, while children who are below the age limit, may get access. Additionally, the lack of accuracy may have a discriminatory effect because the algorithms are often less accurate when analysing the faces of people with darker skin, and especially women.[105]

4.4.3. Age declaration

Age declaration means asking a person to disclose their age, for example when registering an account with a service provider, or when accessing a service or webpage. This is used by many digital service providers today. Age declaration is one of the least intrusive age assurance mechanisms, as it does not require the surveillance of users over time, nor does it increase the risk for digital exclusion.

The presence of an age declaration system signals to children and their parents or caregivers that the content and design of a service is not meant for children under the age limit. This can discourage children from accessing the service. Even if the child does access the service despite the age limit, they may be better mentally equipped to access the website, because they know that they are in an unsafe space.

Age declaration's ease of circumvention is one of the main critiques of the age declaration measures widely used today. A child, their parents or caregivers can simply declare that the child is older than he or she is, and in this way circumvent age gates or other child specific measures.

Although age declaration systems are quite easily be bypassed, the technology can still be useful to protect children and adolescents online. For example, 20% of Norwegian children aged 9-12 use YouTube even when they are not allowed to do so by their parents or caregivers.[106] One out of five is quite a lot – but for TikTok, Instagram, and Snapchat, which are often touted in public discourse as the most problematic services, the number is reduced to 1-2%. It's worth keeping in mind that 90% of children aged 9-12 are allowed to use YouTube,

---

[104] "Online age verification and children's rights", EDRi et al. (2023). https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf and "Mandatory age verification for pornography access: Why it can't and won't 'save the children'", Stardust, Obeid, McKee, Angus (2024). https://journals.sagepub.com/doi/epub/10.1177/20539517241252129

[105] "Ban Biometric Mass Surveillance", EDRi (2020). https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

[106] "Foreldre og medier 2024: Delrapport: Foreldres regulering av barnas mediebruk", Medietilsynet, p. 28. https://www.medietilsynet.no/globalassets/publikasjoner/foreldre-og-medier-undersokelser/2024/delrapport-2-foreldreregulering-av-barnas-mediebruk-med-uttak-fra-fom-og-bom.pdf

while the numbers are lower for other services, such as Snapchat (42%), TikTok (32%) and Instagram (12%).[107]

This illustrates that most of the children who bypass age declaration measures do so with their parents or caregivers' endorsement. Therefore, the solution may not lie with increasing the technical barrier for the child, but rather reducing the social pressure to be present online and the endorsement rate of parents or caregivers. The reasons why many parents allow their children to access social media platforms despite the age limits are many-faceted, and relate for example to a fear of social exclusion. Parental controls, legitimate age limits and other ways to assist parents and caregivers in keeping children safe online is discussed further in chapter 5.2.

More research may be necessary to understand how age declaration measures can be introduced to families in a way that makes it less likely that children circumvent it. Many children want to be safe in online spaces, and it may be possible to leverage this to increase the chance that they are truthful. When age declaration is combined with other measures such as privacy and safety by design and default, and appropriate parental or caregiver supervision, it can become an effective and less invasive measure.

4.5. Principles for legitimate age assurance

Policymakers must take a holistic approach to the protection of children's rights online. This includes considerations about *whether* to ban children from online spaces, which is a very complicated and multi-faceted question. It also includes considerations about *how* to do it, should one find that it is indeed necessary to ban children from the online spaces.

There are various ways to employ age assurance. Notably, the more difficult an age assurance method is to circumvent, the more risks the age assurance method likely holds for children's and consumers' rights. This has an important implication for when the different measures are necessary and proportional; the more stringent age assurance methods should only be considered if other measures have been considered, tested and found lacking.

There are many aspects to consider in terms of the necessity and proportionality of introducing the different age assurance measures. For example, it is worth keeping in mind that age assurance methods cannot be limited only to children. The measure requires that everyone is subject to the same age assurance and its associated risks, which raises the bar for proportionality.

---

[107] "Foreldre og medier 2024: Delrapport: Foreldres regulering av barnas mediebruk", Medietilsynet, p. 26. https://www.medietilsynet.no/globalassets/publikasjoner/foreldre-og-medier-undersokelser/2024/delrapport-2-foreldreregulering-av-barnas-mediebruk-med-uttak-fra-fom-og-bom.pdf

The necessity and proportionality of age assurance methods are also affected by the way the services are design. If targeted measures are implemented, addressing specific risks and practices such as the use of addictive mechanisms or surveillance-based advertising, this could reduce the risks associated with the service. Such measures should not be limited to what is conventionally thought of as social media platforms but should be horizontal and apply equally to for example educational platforms or connected toys. For any service, this would affect whether age assurance measures are proportional.

It is also important to keep in mind what issues one wants to address by introducing invasive technical measures. If age assurance tools are not suited or appropriate to solve the stated problems, or leave major loopholes such as means of circumvention, other solutions must be considered instead.

All of the existing methods for age assurance except age declaration introduce at least some risks for children's and other consumers' rights. Age assurance should only be used in compliance with existing laws. These laws create a framework for legitimate age assurance with a risk- and rights-based approach that thoroughly considers the rights of the child.

Any acceptable verification mechanisms must:

- Be used only when strictly necessary and proportionate.
- Be accessible by everyone, so that individuals and groups above the age limits are not excluded from services that they may rely on. This includes ensuring that people retain a right to a physical ID, and that those above the age limit without access to digital ID are not excluded.
- Not be overly burdensome for those who do not want or do not have the means to verify their identity.
- Avoid chilling effects such as discouraging or preventing children and adolescents from seeking information related to education, health, etc.
- Comply with relevant laws and technical standards,[108] such as the strict requirements set forth in the GDPR.
- Not provide any information to the service provider other than a yes/no, and not facilitate access to any third parties (including parents and caregivers).

[108] See for example "Workshop Agreement: Age appropriate digital services framework", CEN and CENELEC (2023). https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

- Not log or otherwise register usage beyond what is needed to verify the subject's age, and not link information such as internet activity to the subject's identity.

- Not allow the processing of biometric or biometric-based data.

- Be subject to strict security requirements and vetting from independent third parties.

- Not involve ISP-level filtering of the internet or similarly invasive anti-circumvention measures.

- Not lead to the introduction of increasingly invasive surveillance to counter circumvention tactics.

- Include easily accessible and efficient complaint mechanisms in the case that a person's age, whether child or adult, is wrongly identified or estimated.

- Include risk assessments and mitigation measures regarding possible exclusionary and/or discriminatory effects, with particular focus on vulnerable individuals and groups.

5. Measures that are necessary to protect children online

This report has provided an overview of the risks children face online today, which in total amounts to a wholly unsustainable situation. Children should not be exploited for commercial purposes in any area of their daily life, such as when they play, connect with friends, participate in political or other discussions online, or study.

However, it is important to keep in mind that the toxic traits we have outlined, and that currently permeate the digital environment, are not inherent features of social media or the internet. As a society, we can choose to change these features and provide children and adolescents with services that are rights-respecting – and even rights-enhancing.

There is no one-size-fits-all solution to protecting and empowering children in the digital sphere. Instead, governments must take a holistic and cumulative approach to protecting children's rights online. This includes the use of both hard, legal measures, and softer governance measures such as guidelines. In the following sections, we provide a number of recommendations.

5.1. Demand a digital environment that is rights-respecting

The digital environment is currently in poor shape, leaving consumers and children at great risk of exploitation. The silver lining is that many of the harmful practices that have been outlined in this report are regulated through laws that already exist and are applicable. At the EU level, this includes laws such as the General Data Protection Regulation (GDPR),[109] Unfair Commercial Practices Directive (UCPD),[110] Digital Services Act (DSA),[111] and Audiovisual Media Services Directive (AVMSD).[112] At the national level, sector specific laws also protect children, for example the Norwegian Education Act.[113]

The laws apply to different entities and contexts. For example, the UCPD applies to all traders who engage in business practices, the GDPR applies to all processing of personal data, whereas the DSA contains rules that target either all online platforms, or are sometimes limited to the very large online platforms. All the different laws must therefore be enforced in combination to tackle harms in different contexts and from different entities. Where the DSA does not apply, the GDPR and the UCPD can serve as safety nets. One of the most important measures is therefore to ensure that relevant enforcement agencies are actively and boldly enforcing existing laws.

There are currently serious limitations in several of the enforcement regimes that exist. Enforcement of the GDPR is notoriously slow, especially in cross-border cases. For many big companies, breaking laws such as the GDPR and the UCPD is profitable, because sanctions are applied too slowly and the fines are insufficient to have a deterring effect. Breaking the law is simply seen as the cost of doing business. Finally, enforcement agencies do not cooperate enough, which can leave children at risk of "falling between the cracks" of enforcement regimes. Improving and strengthening enforcement structures should therefore be at the forefront of any strategy to make the digital environment rights-respecting.

---

[109] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[110] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').
[111] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 000/31/EC (Digital Services Act).
[112] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance).
[113] Lov om grunnskoleopplæringa og den vidaregåande opplæringa (opplæringslova), LOV-2023-06-09-30. Available in Norwegian here: https://lovdata.no/lov/2023-06-09-30.

While many of the risks children face online can be reduced or mitigated by ensuring stable, dissuasive and bold enforcement of existing laws, there are still some legal gaps. For example, consumer law does not sufficiently account for consumers' and children's vulnerabilities when they are using digital services. Ursula von der Leyen, President of the EU Commission, has tasked the next Consumer Commissioner to develop a Digital Fairness Act to tackle dark patterns (deceptive design), influencer marketing, addictive design and online profiling.[114] An updated consumer law should provide the final protections children need, through horizontal rules that have a wider scope than concrete, digital legislation such as the DSA that only apply to online platforms – and sometimes only to very large online platforms, meaning platforms with more than 45 million users in the EU.

In the following sections, we will outline how digital services can be changed to become rights-respecting and empowering. We will indicate which laws should be enforced better to improve children's protection online, and if there are legal gaps, we propose targeted updates in the law. We also include recommendations to improve enforcement regimes.

5.1.1 Rights-respecting digital services for all consumers

Many of the harms discussed in this report are harmful for all consumers, not only children and adolescents. Neither children nor adults should be subject to predatory business models such as aggressive commercialisation, toxic content, or addictive mechanisms.

When measures to counter the harmful practices are applied generally instead of specifically to children, companies cannot subject children to harmful practices by arguing that they do not know (or if they ignore) that the user is a child. Therefore, digital environments that are rights respecting for all users, also provide the best protection for children. To this effect, a number of measures must be implemented on digital services through ambitious enforcement of existing laws.

[114] "Mission Letter", Ursula von der Leyen, president of the European Commission (2024). https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf

Accountability and risk mitigation

Very large online platforms[115] must identify, assess and mitigate risks to the fundamental rights of consumers. This should include independent audits and transparency requirements, to ensure accountability and stakeholder involvement. There are several articles in the DSA that are relevant in this context:

- Risk assessments are required by the DSA art. 34 and should be based on the best available information as well as civil society participation.[116] The risk assessments of social media platforms should include the risks identified in this report.

- Risk mitigation measures are required by the DSA art. 35 and should be based on the risks identified and assessed in DSA art. 34. The measures should mitigate risks to the fundamental rights of consumers on their platform. While the very large online platforms are responsible for identifying the appropriate risk mitigation measures, this report provides a range of relevant risk mitigation measures that should be considered.

- Independent audits of the risk assessments and risk mitigation measures are required by the DSA art. 37(1)(a).[117]

- Public audit reports are required by the DSA art. 42(4), which includes the results of risk assessments and mitigation measures that have been implemented. A sufficiently detailed public report will allow civil society organisations to identify gaps in the risks assessments performed by very large online platforms.

Addictive design and recommender systems

This report has outlined a number of risks from the way digital services are currently designed. There are numerous existing laws that can be used to reduce harms related to addictive design mechanisms and toxic recommender systems.

Ambitious enforcement of the DSA art. 35 could require very large online platforms to introduce various risk mitigation measures. As described in section 3, recommender systems are at the core of many of the risks that young people face online today. It follows from this that social media platforms should significantly change their recommender systems. In practice, this means that:

---

[115] The list of designated platforms are available here: "Supervision of the designated very large online platforms and search engines under DSA", EU Commission. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

[116] DSA rec. 90.

[117] See also "Youtube Regrets", Mozilla Foundation (2024). https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf

- Recommender systems based on surveillance and profiling should be turned off by default.[118] The GDPR principles of data minimisation and data protection by design and by default can also be enforced to significantly reduce the harms from personalised recommender systems.[119]

- Platforms should offer an alternative recommender system, as also required by DSA art. 38.

- Recommender systems should not be optimised for engagement,[120] and could instead optimise for quality and content.

- Users should be able to choose what kind of content they would like to see.[121]

- Addictive mechanisms should be toggled off as a default. Addictive mechanisms can be also considered unfair commercial practices under the UCPD.[122]

- Easily accessible and useful user controls. This includes parental controls.

- Content creators should be able to tag posts with content that may be disturbing, so this type of content can be hidden behind content warning. Some users may also want to filter such content away completely.

- There must be sufficient resources for human-controlled content moderation equally applied across all languages offered by the service,[123] to remove illegal content from the platforms. This can also be enforced through the DSA art. 6(1)(b).

---

[118] "Ending artificial amplification of hate & hysteria", Irish Council for Civil Liberties (2023). https://www.iccl.ie/wp-content/uploads/2023/12/Ending-artificail-amplification-of-hate-and-hysteria.pdf
[119] GDPR art. 5(1)(c) and 25.
[120] "Safe by Default", Panoptykon Foundation, People vs. Big Tech (2024). https://en.panoptykon.org/safe-default-panoptykon-foundation-and-people-vs-bigtechs-briefing
[121] "Safe by Default", Panoptykon Foundation, People vs. Big Tech (2024). https://en.panoptykon.org/safe-default-panoptykon-foundation-and-people-vs-bigtechs-briefing
[122] UCPD art. 5 and 8, cf. "Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns", Esposito, Ferreira (2024). https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/addictive-design-as-an-unfair-commercial-practice-the-case-of-hyperengaging-dark-patterns/038CED800E0CAD86EC5B5216E0AA88DD.
[123] "How Big Tech platforms are neglecting their non-English language users", Global Witness (2023). https://www.globalwitness.org/en/campaigns/digital-threats/how-big-tech-platforms-are-neglecting-their-non-english-language-users/

In addition to introducing risk mitigation measures, very large online platforms must provide access to data on their recommender systems to researchers who can contribute to the detection, identification and understanding of risks that recommender systems pose to consumers, and particularly children. This can be enforced through the DSA art. 40.

Platforms should have a high level of data protection by design and by default, including with strict purpose limitation, data minimisation, and fair and lawful processing. This requires strong and ambitious enforcement of the GDPR, particularly art. 5, 6 and 25.

Deceptive design and surveillance-based advertising

This report has shown that there are significant challenges concerning the design of digital services and the use of personal data to target advertising to individuals and groups. The laws that are meant to protect consumers today have a limited effect, and it is necessary to update consumer law to clarify and establish that certain practices should never be allowed. This includes:

- Clarifying the interplay between the GDPR, the UCPD and the DSA, that all regulate deceptive design in different ways.[124]

- Introducing a horizontal ban on deceptive design under the UCPD to ensure protection in cases that fall outside the scope of sector specific laws.[125]

- Introducing prescriptive provisions in the UCPD that can be easily applied by regulators.

- Surveillance-based advertising should be prohibited[126] beyond existing platform-specific bans on the use of special category data and children's personal data in the DSA. A general ban is the best way to protect children.[127]

---

[124] Albeit with the caveat that only practices that are not already covered by the GDPR and the UCPD can be enforced through the DSA, cf. DSA art. 25(2). It remains to be seen which practices, if any, will therefore actually be covered by the DSA.
[125] "Towards European digital fairness", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf
[126] "Time to ban surveillance-based advertising", Norwegian Consumer Council (2021). https://storage02.forbrukerradet.no/media/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf
[127] "I-SPY: The billion-dollar business of surveillance advertising to kids", McCann, New Economics (2021). https://neweconomics.org/2021/05/i-spy

Introduce new legal requirements with horizontal protections

There are structural asymmetries between consumers and service providers in digital markets, which leaves consumers particularly vulnerable.[128] Policymakers must also introduce the following requirements in law, for example through targeted updates of the UCPD:

- Traders'[129] duty of care should take consumers' digital vulnerability into account. This means that they should ensure a high level of consumer protection and that consumers' autonomy is not impacted by the way traders design their services.[130]

- Traders should design their services to be fair by design.[131] Default settings must provide consumers the highest level of consumer protection.

- The burden of proof for providing a safe and rights-respecting digital service should be on the traders.[132]

- The introduction of EU-wide regulation of addictive mechanisms, with particular attention to how such mechanisms affect children.[133] This includes:

    - Ensuring horizontal protections in cases that fall outside the scope of existing legislation.

    - Introducing prescriptive provisions that can be easily applied by regulators, with bans on concrete addictive mechanisms.

5.1.2. Demand that children are protected and empowered

In addition to measures that should be introduced to improve the internet overall, there are many laws that provide children with additional protections. For example, traders should not target children with direct exhortations to buy

---

[128] "EU CONSUMER PROTECTION 2.0 - Structural asymmetries in digital consumer markets", Helberger, Lynskey, Rott, Sax, Strycharz (2021). https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf
[129] UCPD art. 2(b).
[130] "Towards European digital fairness", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf
[131] Ibid.
[132] Ibid.
[133] "Addictive design of online services and consumer protection", European Parliament (2024). https://www.europarl.europa.eu/committees/en/addictive-design-of-online-services-and-/product-details/20230908CDT12141

certain products,[134] and very large online platforms have a duty to mitigate risks to children on their services.[135]

Service providers must ensure that they implement necessary measures to protect and empower children in accordance with the law and be held accountable if they fail to do so. In many cases, service providers should also go further than what they are required to do by law, for example by providing services that are created to be used by children and empower them.

When laws contain provisions that provide additional protections for children, service providers need to know whether individuals accessing their services are children. As elaborated upon in this report, any age assurance method must abide by several requirements to be legitimate, necessary and proportionate. This includes ensuring the data protection and privacy of users, digital inclusivity, and cybersecurity.

Age declaration is associated with few risks and could be an important age assurance tool when used in combination with additional measures. For example, providers of operating systems typically allow devices to be set up as a 'child-friendly device', with associated parental controls. This is essentially based on declaration, where a child or the child's parents or caregivers declare that the user of the device is a child.

Once a device is associated with a child, the operating system provider could share this information with app- and service providers on the device by sending out a signal. The signal would trigger the child protective measures other services providers must put in place, as required by law, while reducing the burden on parents and caregivers to change and micromanage the settings in every app and service.

However, if implemented incorrectly, technical age signals may have a detrimental effect on children's rights. For example, if the signal has the practical effect of banning adolescents from most apps and services or hiding certain types of content, this could affect the child's right to information and freedom of expression. In order to prevent an age signal to turn operating system providers into new gatekeepers with the power, for example to select how the signal works and with whom it is shared, any such on-device age signal must be developed as an open technical standard without licensing restrictions and be free and open source to be used by anyone.

It is important that age signals are implemented as soft technical measures, provide granular settings, and are possible to turn off or be changed according to the situation and needs of the child. Furthermore, it is worth keeping in mind

[134] UCPD annex I, 28.
[135] DSA art. 34 and 35.

that any on-device measures such as age-signals will be ineffective if children access digital services through devices that are not specifically designated as theirs, such as the device of a parent or caregiver.

In addition to the changes that must be made for all consumers, digital services providers must in any case implement a number of child-specific measures to protect and empower children online. This can be ensured through ambitious enforcement of existing laws.

Age-appropriate services

Very large online platforms should assess and mitigate risks to children on their platforms, according to DSA art. 34 and 35.[136]

In addition to the requirements on the very large online platforms, *all* online platforms that are accessible to children must put in place measures to ensure a high level of privacy, safety and security for children, according to the DSA art. 28(1). A strict interpretation of the provision could be crucial to tackle the amplification of advertisements and toxic content based on personal data and addictive techniques.

With this backdrop, online platforms should be required to implement measures such as:

- Age-appropriate tools, information and default settings.
- Recommender systems should not be optimised for engagement,[137] and could instead optimise for quality and children's feedback and explicit signals.[138]
- Addictive mechanisms such as infinite scroll, autoplay, and streaks should not be used for children's accounts.
- Children's personal data should not be exploited for commercial purposes, for example to train commercial AI products. This can also be enforced through GDPR art. 5(1), which requires purpose limitation and data minimisation.

[136] See more about these measures in section 5.1.1.
[137] "Safe by Default", Panoptykon Foundation and People vs. Big Tech (2024). https://en.panoptykon.org/safe-default-panoptykon-foundation-and-people-vs-bigtechs-briefing
[138] "Towards a safer, more private and secure internet for children in online platforms", BEUC (2024). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-074_Submission_to_the_Call_for_Evidence_on_Article_28_DSA.pdf

- Accessible and user-friendly tools to erase children's digital footprint.[139]

- Complaints and notice and action mechanisms should be age appropriate and accessible to children and adolescents. DSA art. 16 also requires that all platforms' notice and action mechanisms should be 'easy to access and user friendly'.

- Sufficient employees that are trained to handle complaints and appropriate interactions with minors. They should be available for questions and to help children, for example if children experience unwanted interactions or content.

Online platforms should also be required to implement default settings that protect children's privacy, safety and security:

- Age-appropriate 'safe search'-filters.

- Private accounts for children, where the content or profile are for example not open to the public.

- Notifications should be reduced to the minimum.

- No tracking of children's behaviour online or offline for commercial purposes.[140]

- No recommender systems based on surveillance and profiling.[141] The GDPR principles of data minimisation and data protection by design and by default can also be enforced to significantly reduce the harms from personalised algorithmic feeds.[142]

- No features that rely on social validation signals (such as like/dislike button).[143]

All digital service providers should perform data protection impact assessments when their services are likely to be accessed by children, in accordance with the

---

[139] See more recommendations here: "Towards a safer, more private and secure internet for children in online platforms", BEUC (2024). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-074_Submission_to_the_Call_for_Evidence_on_Article_28_DSA.pdf

[140] Ibid.

[141] "Ending artificial amplification of hate & hysteria", Irish Council for Civil Liberties (2023). https://www.iccl.ie/wp-content/uploads/2023/12/Ending-artificail-amplification-of-hate-and-hysteria.pdf

[142] See article 5(1)(c) and article 25.

[143] "Safe by Default", Panoptykon Foundation and People vs. Big Tech (2024). https://panoptykon.org/sites/default/files/2024-03/panoptykon_peoplevsbigtech_safe-by-default_briefing_03032024.pdf

GDPR art. 35.[144] This includes implementing risk mitigation measures for any risks to children's data protection rights.

Advertising

In order to curb the proliferation of illegal commercial practices and advertising on digital services, numerous measures should be taken:

- Traders should not target children with direct exhortations to buy products. This can be enforced through the UCDP annex 1, including dissuasive fines.

- Digital services should not target children with deceptive design practices. This can be enforced through the DSA art. 25, the GDPR and the UCPD, as appropriate.[145] For example, digital platforms should not deceive children into choosing privacy-invasive settings.

- Digital platforms should not target advertisements based on profiling at children. This can be enforced through the DSA art. 28(2).

Influencer marketing

For influencer marketing, content and advertising should be much more clearly separated than it is today. Hidden advertising is illegal under the UCPD art. 7(2). To operationalize the prohibitions on hidden advertising, EU-wide disclosure standards should be established. The standards should build upon the DSA art. 26(2),[146] and should include:

- Much larger and more visually prominent labels, for example by taking up half the screen in videos.

- Clear separation between influencers' paid/unpaid content, for example by taking distinct "advertising breaks" in their videos when they advertise a product.[147]

---

[144] See the ICO's guidelines: "Data protection impact assessments", https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/

[145] As mentioned in section 5.1.1, it is necessary with a clarification on the interplay between these laws.

[146] "From influence to responsibility: Time to regulate influencer marketing", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf.

[147] Influencers also run the risk of breaching for example UCPD annex 1 point 11 if their commercial intent is not sufficiently clear.

Influencer marketing also warrants targeted updates in consumer law, for example to demand:

- Additional transparency requirements about who is paying for promoted content, building upon the DSA art. 26(2).

- EU-wide rules on joint liability regimes between influencers, their agencies and traders, to create accountability across the influencer value chain.[148]

Introduce new legal requirements with horizontal protections

Children should have additional, horizontal protections beyond the framing as a vulnerable consumer, as is currently the case in the UCPD.[149] Policymakers must therefore also introduce certain new legal provisions through targeted updates of the UCPD, such as:

- A requirement for all traders to consider whether their services appeal to children. If their services appeal to children, they must identify and mitigate risks to children. This should be part of traders' professional diligence and duty of care.[150]

- Provisions that protect children against undue advertising should generally protect them against advertising they are exposed to, rather than advertising targeted at them. This provides a lower threshold for enforcement actions, and stronger protections for children online.

- The threshold for when something is considered 'targeted' at children must be low, to ensure children get the protections afforded to them in laws such as the UCPD.

The UCPD must be amended with more practices that are always unacceptable commercial practices. This will make it easier for companies to draw the red lines for their own commercial practices, and for enforcement authorities to sanction companies that breach the law. This should include:

---

[148] "From influence to responsibility: Time to regulate influencer marketing", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf. In Norway, this is already applicable: "Forbrukertilsynets veiledning om reklame i sosiale medier", Forbrukertilsynet (2024). https://www.forbrukertilsynet.no/lov-og-rett/veiledninger-og-retningslinjer/someveiledning#hvordanmerke

[149] "Towards European digital fairness", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf

[150] UCPD art. 2(h).

- A general ban on advertising targeted to children under the age of 16, or which is exposed to many children under the age of 16.

- A general ban on marketing of foods that are high in fat, sugar or salt.[151]

- EU-wide prohibitions on influencer marketing of gambling, alcohol products, medical products, aesthetic procedures, and other products that can affect children's mental health and well-being negatively.[152]

5.1.3. Improve and strengthen enforcement structures

As noted throughout this report, the internet in general and social media platforms in particular are not lawless spaces. There are many applicable laws in place on both the national and European level. However, many of these laws are currently not being sufficiently enforced, resulting in weaker protections for both children and adults online.

The early days of DSA enforcement are characterized by an ambitious EU Commission, who has launched a myriad of requests for information, for example to TikTok, SnapChat and Instagram about their recommender systems.[153] The Commission has also opened several formal proceedings, and obtained commitments from TikTok to withdraw TikTok Lite Rewards, which included addictive mechanisms.[154] Hopefully, the Commission will continue to enforce the DSA rigorously, including through dissuasive fines.

At the same time, stronger and more efficient enforcement of other laws that regulate digital services is necessary, for example the GDPR, the UCPD and the AVMSD. There are many ways enforcement structures can be strengthened and improved.

Cross-sectoral and cross-border enforcement

Children's rights are spread over many different laws.[155] The enforcement authorities of these laws must have clearly allocated responsibilities, to ensure

[151] "Food marketing to children needs rules with teeth", BEUC (2021). https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-084_food_marketing_to_children_needs_rules_with_teeth.pdf
[152] "From influence to responsibility: Time to regulate influencer marketing", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf
[153] "Commission questions YouTube, TikTok, and Snapchat over recommender algorithms", Gkritsi, Eurativ (2024). https://www.euractiv.com/section/tech/news/commission-questions-youtube-tiktok-and-snapchat-over-recommender-algorithms/
[154] "TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act", EU Commission (2024). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161
[155] In Norway, it is spread over at least 10 different laws: "Nødvendig å styrke barns forbrukervern i digitale medier", Barneombudet, Norwegian Consumer Council (2022). forbrukervern-i-digtale-medier.pdf

that illegal practices against children do not 'fall between the gaps' of enforcement authorities' jurisdictions.[156]

Enforcement authorities must cooperate across sectors. This should include:

- Ensuring that children can easily file complaints against illegal practices. If a complaint is sent to the wrong authority, they should make sure the complaint is sent to the right authority.
- Regularly undertaking coordinated actions across sectors.
- A duty to inform other enforcement authorities if they notice illegal practices that are covered by another enforcement authority's jurisdiction.

Enforcement of children's rights require cross-border cooperation. This means that national enforcement authorities must cooperate with authorities across the EU and the EEA.[157] EU and EEA enforcement authorities should also cooperate with authorities in other countries, such as the US' Federal Trade Commission (FTC) and the UK's Ofcom.

Ensure children can be represented in the legal systems

Many of the business practices outlined in this report are covert, intrusive, and legally and technically complex. Children should not be left to fend for themselves. Instead, they should be allowed to mandate not-for-profit organisations to represent them in proceedings against companies that infringe on their rights. This includes:

- Rights to be represented in collective actions through the Representative Actions Directive,[158]
- Rights to be represented when their data protection rights have been infringed, in accordance with the GDPR art. 80(1).

The business model in question affects millions of children's rights every day. No individual child should have to shoulder the burden of filing complaints against

---

[156] "Too much or too little? Assessing the Consumer Protection Cooperation (CPC) network in the protection of consumers and children on TikTok", Gamito, Micklitz, BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf

[157] Examples of this are the CPC-network and the EDPB.

[158] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance).

some of the biggest companies in the world, on behalf of all other children that are affected by the same practices.

Organisations that meet certain criteria, including being not-for-profit, must therefore be able to lodge complaints against companies that infringe on children's data protection rights in systemic and intrusive ways, without individual children's mandate. This is possible under the GDPR art. 80(2), but requires a national legal basis.

Sanctions

Enforcement authorities must be mandated to use sufficiently dissuasive penalties, including tools such as fines, algorithmic disgorgement[159] and imposing immediate orders to stop illegal practices. This is crucial to dissuade the companies that receive the penalty. Breaking the law cannot be profitable or considered a "cost of doing business".[160]

At the same time, sanctions should also serve to dissuade other companies that engage in similar practices. There are too many traders who employ illegal commercial practices to enforce laws based on private dialogue between enforcement authorities and each commercial entity. If penalties are not dissuasive, enforcement authorities will never manage to stem the tide of illegal practices.

Resources for enforcement authorities

Enforcement of existing laws is a crucial step in improving children's experiences and rights online. This requires that enforcement authorities have sufficient resources, including access to the necessary expertise on for example design and technology. Enforcement authorities must also use technology in a way that makes it possible to scale enforcement.

Self-regulatory approaches have proven insufficient in the digital sphere and introduces a chaotic enforcement structure for children, parents and caregivers. The competences given to self-regulatory bodies should be moved to independent enforcement authorities.

Revise the laws that regulate cross-border cooperation

There is an ongoing legislative process to improve the cooperation on cross-border enforcement under the GDPR. These complaint procedures are currently

[159] "Explaining model disgorgement", IAPP (2023). https://iapp.org/news/a/explaining-model-disgorgement
[160] "Big Tech has already made enough money in 2024 to pay all its 2023 fines", Proton (2024). https://proton.me/blog/big-tech-2023-fines-vs-revenue

very slow, and they are often centred on some of the largest technology companies. The results of the procedures can therefore have an important impact on the privacy and data protection of most, if not all, consumers in the EU and the EEA.

European lawmakers must use this opportunity to update the cross-border rules to ensure:[161]

- Simpler and facilitated lodging of complaints. Complainants, including children, must not be required to substantiate their complaint to the point of it constituting a preliminary legal analysis for the complaint to be valid.

- Reasonable and proportionate deadlines so that the enforcement processes take no longer than 12-18 months.

- The possibility to meaningfully exercise the right to be heard by the parties.

At the same time, the European Commission should revise the Consumer Protection Cooperation Network Regulation,[162] which regulates the cooperation among consumer enforcement authorities, for example of the UCPD.

An updated regulation should include:[163]

- A role for the European Commission to address widespread infringements with a Union dimension, including the power to impose fines.

- A requirement to only close coordinated actions after traders have fully implemented their commitments.

- Procedural rights to entities submitting external alerts about widespread infringements.

---

[161] "GDPR Cross-Border Enforcement Regulation – BEUC's Position Paper", BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-162_Cross-Border_Enforcement_Regulation.pdf

[162] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (Text with EEA relevance)

[163] See more recommendations here: "Strengthening the coordinated enforcement of consumer protection rules", BEUC (2022). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-135_Strengthening_the_coordinated_enforcement_of_consumer_protection_rules.pdf

5.2. Ensure families and governmental agencies are equipped to provide children with age appropriate experiences online

Since it is extremely profitable for digital service providers to exploit children, non-binding instruments like guidelines and recommendations are unsuited to tackle their commercial practices. Conversely, families, parents and caregivers, and public sector agencies do not have commercial incentives to put children in harm's way. Our recommendations therefore include several measures directed at them, such as guidelines, age limits, and governance documents.

5.2.1. Limit the number of children who access digital services even though they are under the age limit

Technically blocking children and adolescents from certain digital services is often at the centre of public discourse about child protection online. This report has shown that introducing age verification on digital services is a complicated and risky measure, because of the effect it can have on children's other rights, the harms associated with most of the currently available technical solutions, and the likelihood that children will use even riskier alternative services.

While age verification may not be the silver bullet many policy makers and enforcement agencies are hoping for, the fact that some digital services are not meant for children under a certain age must still be reckoned with. Governments and companies must put in place measures to reduce the number of children under the age limits who access and use such services.

In Norway, around 50% of 9-year-old children already use social media, despite the platforms' self-imposed age limit of 13 and use of age declaration.[164] Clearly, many children therefore circumvent the platforms' age assurances measures from a very young age. This has convinced many policymakers that hard, technical measures are an absolute necessity – especially given the many risks children and adolescents face on the platforms.

Children sometimes circumvent the age limits of social media platforms without their parents or caregivers' knowledge. For these children, a harder technical barrier may reduce their ability to access the social media platform.[165] However, as outlined in section 4.4.1, children under the age limit usually do not use social media platforms without their parents or caregivers' endorsement, and might

[164] "Barn og Medier 2024: Delrapport: Barn og unges medievaner og tilgang til teknologi", Medietilsynet (2024) p.15. https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2024/delrapport-1_bom_barn-og-unges-medievaner-og-tilgang-til-teknologi.pdf

[165] With the caveat of possible circumvention tactics.

even get their help to bypass the age limit. It is therefore important to reduce the number of parents or caregivers who allow their children to bypass the age limit.

Parents and caregivers often allow their children to use digital platforms even when they are underage, because they fear that their child might be socially excluded if they do not participate online.[166] For example, many school classes create digital groups on social media platforms from an early age. The obvious and immediate risk of social exclusion is considered a much greater risk than the platforms themselves. The lack of coordination and joint decision making among parents and caregivers leads to the lowest common denominator and a race to the bottom.

When parents and caregivers believe that social media is necessary for their children for social reasons, there is an inherent risk that they will continue to allow children to bypass any stricter, technical age gating mechanisms. This issue is reinforced by the fact that many children who are under the age limit, but currently use social media platforms because they have been allowed to do so by their parents or caregivers, would lose access to the platforms if strict age verification was introduced. Therefore, it is not enough to introduce stronger technical barriers; first, the social pressure to be on the platforms must be reduced. This requires that parents, caregivers and children across society believe the age limit for social media is both legitimate and necessary.

The current age limits of social media platforms have so far primarily been decided by the service providers themselves. While the GDPR requires that children be between 13 and 16 before they can consent to the processing of their personal data by social media services,[167] this is not an actual age limit for the services, but rather an age limit for consenting to the processing of personal data. In practice, the GDPR allows parents to consent to the processing of their child's personal data before they reach the age limit for consent. Companies may also argue that they process the personal data of children based on other legal bases than consent,[168] as they have argued after Denmark increased the age limit for consent in 2024.[169] The GDPR's age limits for consent may as such give an indication that such services should not be used by underage users, but is far from a clearcut limit on social media use.

---

[166] "Digitale dilemmaer – en undersøkelse om barns debut på mobil og sosiale medier", Medietilsynet (2023). p. 50. https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2022/230206_digitale-dilemmaer.pdf

[167] Member states are free to decide the exact age limit at the national level.

[168] "Annex C: Lawful basis for processing", ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-c-lawful-basis-for-processing/.

[169] "Hvert andet barn i Danmark er på sociale medier, før de fylder ti år", Medierådet for Børn & Unge (2024). https://medieraadet.dk/aktuelt-fra-medieraadet/2024/maj/hvert-andet-barn-i-danmark-er-paa-sociale-medier-foer-de-fylder-ti-aar

While the current age limits of social media platforms are either unclear or based on companies' self-imposed age limits, there is a lack of clear and factually based guidelines from governments about when children should use social media. A notable and recent addition is the newly published guidelines by the Swedish government.[170] While they do not establish new age limits, they are explicit and clear that children under the age limit should not use social media.

In contrast, the Norwegian government urges parents and caregivers to individually consider whether their children are old and mature enough to use social media.[171] At the same time, government institutions have not properly communicated the risks of the digital services. The risks of social exclusion from not using social media are immediate, whereas the risks of using social media are often much less intuitive and difficult to grasp. Therefore, it is necessary that governments, schools, and other public institutions communicate these risks clearly to children, parents and caregivers through channels such as health stations, kindergarten, schools and libraries.

A legitimate age limit requires that governments find the right balance between children's many rights and interests. After setting this age limit, governments must also explain the reason for the age limit and provide clear guidance to families, schools, and other institutions with responsibilities for and to children. This can lay the groundwork for parents and caregivers, allowing them to decide collectively that their young children are not allowed to use social media. Discrepancies in the communications about the age limit at which governments recommend that parents and caregivers let their children access social media services, serve to weaken the legitimacy of the age limit and should be avoided.

A legitimate age limit must be complemented by practical and functional parental controls, age-appropriate design, and rights-respecting default settings.

Governments must equip families with:

- Legitimate age limits, clear advice, and functioning tools. For example, parents cannot be expected to make individual risk assessments about concrete digital services, that are legally, socially, commercially and technically complex.

[170] "Rekommendationer för en balanserad skärmanvändning bland barn", Folkhälsomyndigheten (2024). https://www.folkhalsomyndigheten.se/nyheter-och-press/nyhetsarkiv/2024/september/rekommendationer-for-en-balanserad-skarmanvandning-bland-barn

[171] As of October 15, 2024. See for example Bufdir's guidelines: "Barn og sosiale medier". https://www.bufdir.no/foreldrehverdag/skolebarn/digital-hverdag/barn-og-sosiale-medier/

- Age-appropriate guidelines, based on the precautionary principle, and could include elements such as:
    - General advice to follow age limits.
    - Which types of digital services children under a certain age limit should not use.
    - The maximum amount of time children at different ages should spend on social media or other digital services.[172]
    - Advice on 'safe search' settings and other settings that are relatively easy to use and efficient.

5.2.2. Parental supervision should only supplement other measures

While it is important that parents and caregivers regulate their children's use of smartphones and digital services, it is unfair to push the whole responsibility over on individual families. There are many reasons for this.

The effectiveness of parental control is reduced as children grow older. By the time they become teenagers, it is extremely limited. Digital competence is not evenly distributed among parents and caregivers – and some children do not have parents or caregivers at all. It is highly problematic if children with digitally competent parents or caregivers are the only ones that are provided protection in the digital sphere.

To ensure basic levels of protection for all children, parental supervision can only be a supplement to other systemic measures, for example by governments, schools and service providers. Policy makers must prioritise demanding companies to change their digital services to make them rights-respecting, with the measures we described in section 5.1. However, implementation of many of these measures will take time. In the meantime, the most efficient tool to protect young children is to reduce the use of the most harmful digital services. Technical parental controls can be a useful tool in this regard.

It is important to keep in mind that certain technical parental controls can also be abused, for example by providing the opportunity to spy on children or removing access to content and apps that is necessary for the well-being of adolescents and teenagers. Such content can for example be access to third party helplines, or information about sexuality, gender or religion. Children and adolescents also have varying domestic situations. For example, being

[172] See for example "Till dig som har barn i åldern 6–12 år", Folkhälsomyndigheten (2024). https://www.folkhalsomyndigheten.se/livsvillkor-levnadsvanor/digitala-medier-och-halsa/till-dig-som-har-barn-i-aldern-612-ar/, only available in Swedish.

dependent on parental controls in violent domestic circumstances, can do more harm than good.

Any measure to protect children through parental supervision, must not lead to undue control of children, especially as the children grow older. Parental control should be carried out with the full knowledge of the child, and parents or caregivers' access and control should loosen up gradually as the child grows older.

While parents and caretakers can try to protect their young children through age-appropriate settings, many of the features they need must be provided by the relevant services providers.[173]

When provided, parental control tools should**:**

- Include defaults and recommended settings for children of different ages.
- Be accessible and easy to use.
- Function across operating systems and devices.
- Be functional.
- Allow parents and caregivers to create separate age-appropriate profiles and accounts for their children, where measures to protect children are implemented as a default.
- Ensure parents and caregivers are not required to have a complete overview and micromanage settings for multiple apps, services or websites, as this is a daunting if not impossible task for most parents.
- Ensure children get information about the way parental controls work in any age appropriate an easily accessible way.

As described above, clear guidance and assistance from public institutions is also key to help parents or caregivers individually and as a group to have a responsible approach to the use of social media among children and adolescents.

[173] This can be considered one of many measures to ensure children's safety, security and privacy under DSA art. 28, and as a risk mitigating measure under DSA art. 35. See more about this in sections 5.1.

5.2.3. The public sector must lead by example

While online service providers have been a primary concern in this report, there are also important changes that must happen in the public sector. For the past 20 years, digital services have been rolled out in schools and other institutions, often without sufficient control over who gets access to the children's personal data and attention. This was turbocharged during the pandemic.[174]

In practice, many of the unscrupulous commercial practices that children are exposed to in their spare time, is also part of their school day. For example, 12-year-old girls are exposed to advertisements for dieting pills on their school device calculators, and students' personal data are reused for unspecified purposes through 'free' apps.[175] A Human Rights Watch report also uncovered that of 163 EdTech products they reviewed in an investigation in 2022, 145 (89 percent) appeared to engage in data practices that put children's rights at risk'.[176]

The low protections afforded to children in schools have at least two important effects; children are exposed to unacceptable risks while they are in school, and schools have a signalling effect to parents and caregivers. Parents and caregivers are unlikely to consider constraints an important measure to reduce risks for young children online, when schools provide iPads and computers without any safeguards.

There are many measures that the public sector can implement to reduce children's exposure to unacceptable commercial and data invasive practice. Governments should for example give schools and other public sector institutions that provide digital services for children:

- A catalogue of digital services, which have been deemed safe from a data protection, privacy and security perspective, and that are free from commercial pressure. It is unrealistic for each school to have the necessary technical competence to do this individually.

- Codes of conduct for relevant public sector institutions, to provide a high level of information security and data protection.[177]

---

[174] "An ed-tech tragedy? Educational technologies and school closures in the time of COVID-19", UNESCO (2023). https://www.unesco.org/en/articles/ed-tech-tragedy-educational-technologies-and-school-closures-time-covid-19

[175] "Ditt personvern – vårt felles ansvar", NOU 2022:11, Personvernkommisjonen (2022) https://www.regjeringen.no/contentassets/e4c60a6c51b147628b2c2e55db7e08e3/no/pdfs/nou202220220011000dddpdfs.pdf

[176] "How Dare They Peep into My Private Life?", Human Rights Watch (2022). https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[177] "Læring, hvor ble det av deg i alt mylderet?", NOU 2023:19, The Expert Group for Digital Learning Analysis (2023). https://www.regjeringen.no/no/dokumenter/nou-2023-19/id2982722/?ch=5%22%20\l%20%22kap13

Governments should require school owners and other public sector institutions that provide digital services to children to:

- Provide content filters on school devices and school networks. This measure is especially relevant for younger children. When filtering content, schools or filter providers must be mindful of children's right to access to information, especially as they grow older.

- Install advertisement blockers on school devices and ensure there are no advertisements on digital services provided to children through schools or other public institutions. The advertisement blockers must apply both on school grounds and at home, if the children are expected to bring the devices home. This will reduce the commercialization of the services, and the privacy risks related to the placement of the advertisements. Children should not be treated as consumers while they are in school or when using other services provided by the government.

- Facilitate discussions and offer clear guidance and rules to students and parents about the use of digital technologies.

5.2.4. Empowerment of children and adolescents

Finally, it is key to also give children and adolescents the tools to best prepare them for the challenges they meet when they are online, for example through education. So far this has often been the only solution policy and decision makers have focused on, placing the burden of responsibility on children and adolescents themselves to deal with the vast challenges that social and other digital media can pose. This approach has clearly failed and is utterly inadequate.

However, if policy and decision makers manage to have a holistic approach to dealing with the challenges, as outlined in this report, then there is also a strong argument to ensure that digital competence and empowerment is a part of this holistic approach. A broad approach to teaching about media literacy, should include learning about online business models, privacy, data protection, security, commercial practices, bullying, mental health, unwanted attention, mis- and disinformation and more. Involving and teaching children and adolescents should start at an early age and be adapted accordingly. Schools and public institutions play a key role.

forbrukerradet.no

FOR MORE INFORMATION:
Finn Lützow-Holm Myrstad, director of Digital Policy
Norwegian Consumer Council
finn.myrstad@forbrukerradet.no