

cerre



**A FRAMEWORK FOR
ALIGNING BUSINESS
INCENTIVES TO PROTECT
CHILDREN ONLINE**

REPORT

October 2026

Jan Krämer

Michèle Ledger

Sonja Herrmann



As provided for in CERRE's bylaws and procedural rules from its “Transparency & Independence Policy”, all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Apple, Agcom, CnaM, Microsoft, Ofcom, OpenAI, Snap. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

© Copyright 2026, Centre on Regulation in Europe (CERRE)

info@cerre.eu – www.cerre.eu

Executive Summary

Digital services and platforms have become an integral part of children’s lives and can offer substantial benefits. They provide new opportunities for learning and creativity, facilitate access to information and knowledge, support the development of digital skills, and enable children to maintain social relationships and participate in communities. At the same time, there is growing awareness that these opportunities are accompanied by potentially significant harms. **The policy challenge is therefore not simply to restrict children’s access to digital services, but to preserve and enable their benefits while reducing the risks and harms that children may encounter in the digital environment.**

A proposed framework for analysis based on business models

This report develops a novel framework for understanding, and ultimately regulating, the ways in which digital services create risks of harm for children online. Much of the current policy debate, including proposals for outright national bans on social media use by minors, focuses on restricting children’s access to individual services or on prohibiting specific harmful design features, such as infinite scrolling, autoplay, beauty filters, or loot boxes. This report takes a different approach and provides new foundational thinking meant to advance and reshape the debate on the topic rather than providing a definitive conclusion. Our main idea is that **regulation should not be retrofitted, cataloguing individual harmful service features, but rather trace the harms back to and address them at their root cause: the underlying financial and business incentives that create potentially harmful design choices by the service provider.** Online harms to children are conceptualised not as isolated design flaws but as structurally anticipated byproducts of a service’s pursuit of profit maximisation. The greater the financial gain a service derives from a risk-inducing feature, the stronger its incentive to tolerate, and even to encourage, the harm that the feature creates. Regulation that targets individual features without addressing this underlying incentive structure is therefore likely to remain a game of whack-a-mole, as providers redesign services to act on the same financial incentive through different means.

Building on the OECD’s well-established five-category (“5C”) typology of children’s online risks—consumer, content, conduct, contact, and cross-cutting risks—the report identifies seven business model dimensions that map systematically onto these risk categories: a service’s reliance on usage duration and its reliance on opaque monetisation strategies (both linked to consumer risk), its reliance on the availability of harmful content (content risk), its reliance on user-generated content (conduct risk), its reliance on inter-user interaction (contact risk), and its reliance on the collection of personal data and on experimental technology such as generative AI (both linked to cross-cutting risk).

For each dimension, the report proposes a guiding question that captures the financial incentive at stake: for instance, how much a service would lose in revenue if it disallowed user-generated content, or how much it benefits from keeping a user online for one additional minute. Applying these guiding questions to a given service, existing or yet to be developed, yields a **qualitative risk profile** that indicates how much regulatory scrutiny that service should receive, independent of how the service happens to be categorised under existing law. Applied to three prototypical business models—a subscription-financed streaming service, an advertisement-financed social networking service, and a subscription-financed AI assistant—the framework shows that advertisement-financed social networking services generate by far the highest risk profile, precisely because advertising, opaque

monetisation, user-generated content, open interaction, and data collection reinforce one another within the same business model.

The report further highlights that access to any single online service is typically nested within a broader ecosystem of providers, layered across the device, an intermediary (such as an app store, browser, or search engine), and the end-service itself. Each layer pursues its own revenue-maximising logic and therefore carries its own risk profile. Because risks accumulate cumulatively across this stack, and because the misalignment between profit maximisation and child protection is strongest at the end-service layer and weakens with distance from it, **the report argues that control functions such as age verification are best exercised as far upstream as possible rather than left to the end-service provider**, whose revenue such controls most directly and immediately reduce.

Policy Recommendations

On this basis, the report puts forward **eight recommendations** for realigning the economic incentives of digital service providers with the protection of children online.

Recommendation 1 sets out the report's overarching principle: **regulatory oversight should scale with the risk that a service's business model creates for children**. Because the seven risk-inducing business model dimensions tend to reinforce one another, oversight should tighten as a service's overall risk profile rises, up to and including restrictions on how, or even whether, a given business model may serve children at all. As a starting point for discussion, the report proposes to treat a service as "high-risk" once it scores "high" on at least three of the seven dimensions, while calling for further research to develop more quantitative thresholds over time.

Three of the remaining recommendations **apply to all services, irrespective of their individual overall risk profile**, because they target financial incentives that translate most directly and universally into harm.

- **Recommendation 2** calls for **strict limits on advertising to children**: very young children (under 13) should not be exposed to advertising at all, while age-appropriate quantitative and qualitative limits—inspired by, but extending beyond, the existing rules for linear television under the Audiovisual Media Services Directive—should apply progressively to adolescents, with targeted advertising to minors prohibited across all services.
- **Recommendation 3** calls for transparency about how the service is monetised and proposes to set an **end to opaque monetisation strategies directed at children**, including probability-based mechanics such as loot boxes and virtual currencies that obscure real-world cost, in favour of transparent, clearly communicated pricing and fixed contract terms.
- **Recommendation 4** calls for the **collection of children's personal data to be strictly minimised**: providers should be barred from prompting children, or their legal guardians, to consent to data collection beyond what is strictly necessary to deliver the service, and from further processing, for commercial purposes, any personal data collected to protect minors.

The remaining four recommendations apply specifically to services that meet the report’s “high-risk” threshold.

- **Recommendation 5** calls for **regular, independent external audits of high-risk services’ age assurance and content moderation practices**, with a mandate to transfer these functions to a neutral third party—potentially anchored at the device layer, drawing on lessons from auditor-independence rules in the financial industry—where audits reveal persistent shortcomings.
- **Recommendation 6** calls for **restricting the ability of children to upload user-generated content** on high-risk services, with restrictions on the reach and vividness of that content eased gradually as children mature.
- **Recommendation 7** calls for **restricting inter-user interaction between children and other users, including peers and strangers, on high-risk services**, again to be relaxed gradually as children grow older, in order to guard against grooming and other contact-related harms.
- **Recommendation 8** calls for **limiting children’s exposure to experimental technologies, such as generative AI, on high-risk services**, with particular attention to features explicitly designed to foster emotional dependence or attachment, which the report argues should never be permitted for children regardless of age.

Across all eight recommendations, the report favours a developmental approach, consistent with the recommendations of the EU’s Special Panel on Child Safety Online: **restrictions should be calibrated to a child’s age and gradually eased as the child matures and gains digital literacy, rather than imposed as blanket, outright bans**. The report argues that this targeted, incentive-based approach is likely to be more proportionate, and ultimately more effective, than banning entire categories of service for minors, since outright bans tend to create a strong desire among children to circumvent them, often pushing them toward less regulated and less safe alternatives.

Implications for the EU digital rulebook

Assessed against the current **EU legal framework**, the report finds that existing rules—chiefly the Digital Services Act (DSA), the Audiovisual Media Services Directive, the GDPR, and the Unfair Commercial Practices Directive—**already address parts of these recommendations, but only in a piecemeal, indirect, and largely service-specific manner**. The DSA, in particular, embodies a risk-based logic similar in spirit to the report’s framework, in that obligations increase with a platform’s reach, but it ties those obligations to a service’s user base and legal categorisation rather than to the underlying business model. As a result, entire categories of services that the report’s framework identifies as high-risk—including large parts of the video game and AI assistant sectors—run the risk of falling outside the DSA’s scope entirely. The report therefore concludes that simply reforming or amending the DSA would not be a sufficient response to the gaps identified: because the DSA’s scope is confined by design to online platforms and to very large platforms and search engines, it cannot be stretched to reach the full range of business models that the report’s framework shows to generate comparable risks to children.

The report concludes that **new, dedicated EU-level legislation on the protection of minors online is needed**. In the spirit of simplification of the current legislative framework, **this would replace the current rules on the protection of minors that are contained in sector-specific legislation (in particular Article 28 of the DSA)**. Such legislation should preferably take the form of a directly applicable Regulation, organised around the risk profiles of business models rather than around fixed and inevitably narrower service categories, and should be supplemented by legally binding technical standards capable of being updated through delegated or implementing acts as new business models and technologies continue to emerge. It should also replace the current framework's reliance on broad, principle-based obligations and slow, ex-post enforcement with clearer ex-ante rules and prohibitions, so that children are not left exposed to harmful practices for the duration of lengthy European Commission investigations and any subsequent litigation.

Although the proposed EU Kids Act provides such a new, dedicated EU-level legislation to protect minors, it differs significantly from our proposal and was made public only after the thoughts and recommendations in this report had already been developed. At the time of writing, the proposed EU Kids Act is limited to a specific set of services, which are deemed high risk by definition, and for which the proposal requires a safe service design by default. As it stands, **the proposed EU Kids Act, however, does not address or curtail the firm's business incentives that have led to the risky and unsafe design choices in the first place nor does it provide a framework through which the risk of new service types could be addressed in the future**. The EU Kids Act and our proposal are therefore fundamentally different.

The **one area in which the report considers its recommendations to be adequately addressed by a legislative initiative already in progress is opaque monetisation: the upcoming Digital Fairness Act (DFA)** is expected to tackle dark patterns, virtual currencies, loot boxes, and related manipulative monetisation and subscription practices, including as they affect minors. The report therefore recommends that Recommendation 3, on the transparency of monetisation strategies, be implemented through the horizontal DFA rather than through a separate, dedicated legal instrument on the protection of minors, while all other recommendations should be embedded in that dedicated new instrument.

Table of Contents

EXECUTIVE SUMMARY	1
TABLE OF CONTENTS.....	5
1. INTRODUCTION	7
2. ONLINE RISKS AND HARMS FOR CHILDREN	9
2.1. CONSUMER RISKS	9
2.2. CONTENT RISKS	10
2.3. CONDUCT RISKS.....	10
2.4. CONTACT RISKS	10
2.5. CROSS-CUTTING RISKS	10
3. CONNECTING ONLINE BUSINESS MODELS TO RISKS	12
3.1. INCENTIVES FOR FIRMS TO CREATE RISKY ONLINE SERVICES	12
3.2. A FRAMEWORK TO CONNECT BUSINESS MODELS TO RISK	14
3.2.1. BUSINESS MODEL DIMENSIONS RELATING TO CONSUMER RISKS	15
3.2.2. BUSINESS MODEL DIMENSION RELATING TO CONTENT RISKS	19
3.2.3. BUSINESS MODEL DIMENSION RELATING TO CONDUCT RISKS	20
3.2.4. BUSINESS MODEL DIMENSION RELATING TO CONTACT RISKS	22
3.2.5. BUSINESS MODEL DIMENSION RELATING TO CROSS-CUTTING RISKS	23
4. PUTTING THE FRAMEWORK TO USE	28
4.1. SUBSCRIPTION-FINANCED VIDEO STREAMING SERVICE WITH PREDOMINANTLY FIRST-PARTY CONTENT	28
4.2. AD-FINANCED SOCIAL NETWORKING SERVICE	29
4.3. SUBSCRIPTION-FINANCED AI ASSISTANT	30
4.4. INTERMEDIATE CONCLUSIONS	31
5. SERVICE ACCESS LAYERS AND SERVICE ECOSYSTEMS.....	33
5.1.1. RISKS TEND TO ACCUMULATE ALONG THE SERVICE LAYERS	34
5.1.2. MISALIGNED INCENTIVES TEND TO BE STRONGER AT THE END-SERVICE LAYER.....	34
5.1.3. ECONOMIC INCENTIVES TO PROPERLY EXERCISE CONTROL FUNCTIONS FOR CHILD PROTECTION, SUCH AS AGE VERIFICATION, ARE BEST ALIGNED AT THE DEVICE LAYER.....	35
6. EU DIGITAL RULEBOOK.....	37
6.1. CURRENT RULEBOOK.....	37
6.2. OUTLOOK.....	40
7. POLICY RECOMMENDATIONS	42
7.1. GENERAL FRAMEWORK	42
RECOMMENDATION 1: (RISK-BASED OVERSIGHT).....	42
7.2. RULES APPLICABLE TO ALL SERVICES, IRRESPECTIVE OF THEIR OVERALL RISK PROFILE	45
RECOMMENDATION 2 (USAGE DURATION)	45
RECOMMENDATION 3 (OPAQUENESS OF MONETISATION)	47
RECOMMENDATION 4 (DATA COLLECTION)	50
7.3. RULES APPLICABLE TO HIGH-RISK SERVICES.....	51
RECOMMENDATION 5 (ACCESS TO HARMFUL CONTENT)	52
RECOMMENDATION 6 (USER-GENERATED CONTENT).....	56

RECOMMENDATION 7 (INTER-USER INTERACTION)	57
RECOMMENDATION 8 (EXPOSURE TO EXPERIMENTAL TECHNOLOGY)	58
7.4. SUMMARY	59
<u>8. CONCLUSIONS</u>	<u>61</u>
<u>9. REFERENCES</u>	<u>62</u>
<u>ABOUT CERRE</u>	<u>69</u>
<u>ABOUT THE AUTHORS</u>	<u>70</u>

1. Introduction

Digital services and platforms have become an integral part of children's lives and can offer substantial benefits. They provide new opportunities for learning and creativity, facilitate access to information and knowledge, support the development of digital skills, and enable children to maintain social relationships and participate in communities. Digital environments can also provide important spaces for self-expression and the exploration and formation of personal and social identities (OECD, 2025). At the same time, there is growing awareness that these opportunities are accompanied by potentially significant harms. Children may be exposed to harmful or inappropriate content, cyberbullying and other abusive behaviour, privacy risks, and platform features that can contribute to problematic patterns of use or adversely affect their well-being (UNICEF, 2025; Fegert & Melchior, 2026). **The policy challenge is therefore not simply to restrict children's access to digital services, but to preserve and enable their benefits while reducing the risks and harms that children may encounter in the digital environment.**

Existing EU instruments such as the Digital Services Act and the Audiovisual Media Services Directive address some of these risks, but obligations remain fragmented and inconsistent: services that share similar underlying business models and generate similar harms—online games and social networking services, for example—are sometimes regulated differently. Much of the current policy debate, including national social-media bans for young users, focuses on restricting access and prohibiting certain design features rather than addressing the structural drivers of harm. The proposed **EU Kids Act**¹, which was made publicly available only after the thoughts and recommendations in this report had been developed, seeks to reconcile the fragmented and inconsistent regulatory landscape, but still does so by regulating only specific service types and by focusing on risky design features.

This **CERRE report develops a novel framework that maps the dimensions of digital business models to the risks of creating online harms for children.** Our aim is to shift the analytical focus away from harmful individual design features and towards the economic incentives that are the root causes that give rise to harmful features. In our analysis, we focus on harms arising from digital services and content harms of legal content, thereby excluding harms arising from physical products and harms from content that is illegal for all age groups.

Building on the established taxonomy of consumer, content, conduct, contact, and cross-cutting risks, we identify the **business-model characteristics that systematically generate each risk type.** These characteristics include a model's reliance on usage duration, on opaque monetisation strategies, on the availability of harmful content, on user-generated content, on inter-user interaction, on extensive personal data collection, and on experimental technology. For each, we propose a lead question that captures the financial incentive at stake, for instance, how much a service benefits financially from keeping a user online one additional minute. Applying these questions yields a risk profile for any given service, which should give an indication of how much regulatory scrutiny that service should receive.

The framework developed in this report is meant to guide policymakers and regulators to assess the risks that are inherent to a digital service – whether already existing or yet to be developed. However, it may also inform the service providers themselves about the drivers of risks for their

¹ Proposal for a Regulation of the European Parliament and of the Council: EU Kids Act - 'EU Keeping Internet Digital Spaces Accountable and Trustworthy'. COM(2026) 681 final. <https://ec.europa.eu/newsroom/dae/redirection/document/132530>.

chosen business model. It presents foundational new thinking on the topic, and should therefore be seen as a starting point of the debate, rather than a definitive conclusion, on appropriate and proportionate regulation of digital services in order to provide a safer online environment for children. We also acknowledge that any proposal for regulating digital services in an effort to better protect children online would need to be complemented by a comprehensive strategy with regard to education and digital literacy, both for children and their guardians (see, e.g., UNESCO 2026).

We recognise that online harms to children are typically byproducts of a chosen business model rather than deliberate goals: the greater the financial gain a service derives from risk-inducing features, the more willing it is to tolerate the harms those features create. We further take into account that access to the **online environment is layered**—across device, intermediary, and end-service layers, so that risks for harm accumulate within an ecosystem of actors. The strongest potential misalignment between the business model and the incentives to protect children online can arise at the end-service layer. Therefore, we argue that for high-risk services, access and control functions, such as age verification, should not be done by the very service provider at the end-service layer for whose service access is controlled.

Rather than advocating bans, the framework allows us to derive recommendations on how the business models themselves need to be adapted—and how regulation can be made more coherent and risk-proportionate—so that incentives are realigned towards better protection of children. The aim is an incentive-compatible, ecosystem-wide approach that holds services with comparable business models and harms to comparable standards and identifies and addresses financial incentives as the root causes of online harms for children, rather than specific service-features (such as addictive designs and algorithms), which are just the symptoms that emerge from these incentives.

We evaluate our recommendations against the current legal framework aimed at protecting children online and identify gaps that could be filled in future legislation, such as the Digital Fairness Act.

The remainder of this report is structured as follows. Next, we briefly introduce the OECD risk taxonomy against which we will map business model features. In Section 3, we derive our framework, connecting revenue generation to the five risk categories. We do so by presenting seven dimensions that each help assess a firm's risk profile with a distinct guiding question. In Section 4, we exemplify our framework by applying it to three prototypical digital business models. In Section 5 we discuss the implications of our framework recognising that access to an individual service is typically nested within an ecosystem of other services. Finally, in Section 7 we derive policy recommendations and relate them to the existing EU regulatory framework for protecting children before we conclude in Section 8 by summarising the legal gaps that should be addressed in future regulation dedicated to the protection of minors.

2. Online Risks and Harms for Children

In order to be able to map business model characteristics to online risks for children, we first need to adopt an understanding of online risks and harms for children. We focus on the specific harms for children arising from digital services and harms of legal content, thereby excluding harms arising from physical products and harms of content that is per se illegal for all age groups.

In line with the international legal definition established by the United Nations Convention on the Rights of the Child (United Nations General Assembly, 1989), we refer to a “child” as an individual under the age of 18. Furthermore, we use “minor” interchangeably with “child” in order to align with the terminology used by the report by the Co-Chairs of the Special Panel on Child Safety Online, appointed by the President of the European Commission Ursula van der Leyen (Fegert & Melchior, 2026).² Where useful, we further distinguish between ‘very young users’ (under the age of 13) and ‘adolescents’ (ages 13 to 18).

We adopt the **well-established OECD’s (2021) 5C-typology to categorise digital risks for children** into five distinct categories based on how they experience being online. The OECD typology was created with children and their specific vulnerabilities in mind. Nevertheless, most, if not all, of the risks from this typology should in principle also apply to adult users.

While online risks may apply to users of all ages, it is important to recognise that children are in many ways more vulnerable than adults and may experience more severe harms from any risk (Smahel et al. 2020). At the same time, not every harm will be equally severe for every child, as there are vast differences between different children’s cognitive ability and vulnerability, depending on their age and individual experiences (Livingstone & Smith, 2014). Generally, risks are more pronounced for the younger child, albeit factors such as susceptibility to peer influence and psychological vulnerability can be highest for adolescents (Fegert & Melchior, 2026, pp. 41-46). Therefore, and in line with the report by the Special Panel on Child Safety Online (Fegert & Melchior, 2026), we generally support a developmental approach to child safety online, whereby the regulatory framework should differentiate according to the age of the child, where the age serves as a proxy for a child’s development. As a child matures, the exposure to risks may gradually be increased so that by the time the child becomes an adult, s/he has been able to learn how to cope with an inherently risky online environment. Notwithstanding, Fegert & Melchior (2026, pp. 45-47) also point to the fact that with age, the exposure to digital services tends to increase, while parental control tends to decrease, creating a “critical zone”, especially around the age of 13, where children become adolescents.

The five risk categories outlined by the OECD (2021) are as follows.

2.1. Consumer Risks

Consumer risks refer to the **commercial dangers children face as participants in the digital economy** (OECD 2021). These risks typically arise when children are targeted as inexperienced and credulous participants in commercial interactions. This could manifest in blurred pricing through bundling or virtual currencies, manipulation through targeted advertisements or the exposure to manipulative or

² In contrast to Fegert & Melchior (2026), we use “children” for all users under the age of 18, whereas they refer to children exclusively to users under the age of 13.

harmful marketing messages. It may not be directly transparent to the child whether, with what and how much they pay and what they get in return. Furthermore, the more time a child spends online, the more monetisation opportunities are likely to arise, for example by exposing the child to more advertisements or presenting them with in-app purchase options, such as for game enhancements. In this report, we specifically focus on consumer harms that arise with an advertisement-based business model as such, irrespective of the content of advertisements, which, of course, can also be harmful to children (Baldassarre, Ragone & Tibido, 2025).

2.2. Content Risks

Content risks occur when a **child passively receives, engages with, or is exposed to potentially harmful material that is broadcast or available to internet users** (OECD, 2021). This material can be disseminated in various ways, e.g., through content feeds on social networking apps, sent in private chats in a one-on-one conversation or displayed in advertisements or on websites. Content can take the form of different media, i.e., words, symbols, pictures, or videos. Each of these can present the content with an increasing “vividness” through higher sensory depth, i.e., higher amounts of data transmitted via the technological structure of the medium (Steuer 1992). That means that through a video more visual, auditory, and contextual information is immediately transmitted as compared to a simple textual comment. As recognised by the OECD (2021), content is harmful when it is created with hateful or offensive intent, about psychologically distressing matters, and includes misinformation, disinformation or illegal material.

2.3. Conduct Risks

Conduct risks occur when **children act as actors in peer-to-peer exchanges in which their own behaviour makes them vulnerable to harm** (OECD, 2021). Such behaviours include children initiating aggressions with hateful or harmful intent, actions of an illegal nature, e.g., distributing explicit photos of themselves or of others without their consent or sending credible threats. Such behaviour is medium mediated, which means that content in any form, i.e., words, symbols, pictures, songs or videos, is needed to facilitate this conduct risk. To distinguish this from the content risk dimension, the conduct risk is rather about the process of creating such content and how it is shared rather than the perception of it.

2.4. Contact Risks

Contact risks occur when **children become victims of an interaction with harmful intent** (OECD 2021). Contrary to the conduct risk, here the child is the victim by definition, rather than the initiating party. These interactions can be hateful encounters with the goal to offend, expose or cause harm to a child, or per se illegal encounters, e.g., related to sextortion, grooming or blackmailing.

2.5. Cross-Cutting Risks

Cross-Cutting risks are **overarching risks that transcend the previous four risk categories**. This category is concerned with data collection, information privacy but also with the general risk of online technologies that can have arbitrary effects if not sufficiently tested. Any general physical and

psychological health risk of being online is also recognised. This includes heightened anxiety or sleep deprivation symptoms as well as addiction-like behaviours (Munzer et al. 2024).

3. Connecting Online Business Models to Risks

3.1. Incentives for Firms to create Risky Online Services

Commercial online services evaluate their actions foremost from a business logic, intending to maximise profits. Whenever children are contributing to these profits, the firms may have a conflict of incentives **between their business models and protecting children** from risks and harms online. For example, an advertising-based business model creates incentives for firms to keep users online as long as possible and to collect as much data about them as possible so more ads can be shown and ad targeting can be optimised. This creates a conflict with the incentive to mitigate (cross-cutting) risks that arise from data collection and spending too much time online.

While many commercial online services nominally deploy safety mechanisms for minors (e.g., screen time controls, age verification and limited commercialisation), these measures work directly against the financial incentives of the firm, explaining why adherence to such safety mechanisms may be particularly low and not effective in many instances.

We conceptualise online risks not as design flaws but structurally integrated byproducts of an online service's value proposition and profit maximisation incentive. The central premise of this report is that **when profit maximisation depends on metrics that inherently conflict with child safety, service providers face a structural misalignment of incentives for safe service design**. While companies pledge that protecting children online is important to them, that pledge is the more challenging to uphold the more profit is at stake (Engels & Potthoff, 2025; also see Zuboff, 2019). In other words, the higher the financial gains, the stronger the incentive is to “look the other way” with respect to minor protection and the creation of online harms by their service (5Rights Foundation, 2021). It is important to note that the creation of online harms for minors is therefore a byproduct of the firms' business model, and not an aim in itself.

Therefore, we suggest that in order to rebalance economic incentives and incentives to protect children online, effective **regulation should strive to address the root cause that creates harms**, i.e., the commercialisation of online activities of children, and should not just focus on the symptoms of that commercialisation that manifest themselves in unsafe and risky service design features.

For example, service features like “infinite scrolling” and “addictive algorithms” are symptoms of many advertisement-based business models, which have an incentive to keep the user engaged with the goal that the user stays online as long as possible, so more ads can be shown, and more revenue can be generated. Presenting exceptionally engaging content in specific time intervals in an endless feed of content raises curiosity in the user and makes them stay longer on the service in hopes of discovering another piece of content like it (see e.g., Aridor et al., 2024; Beltrán, 2025; Engels & Potthoff, 2025). Attempts to regulate the symptoms (e.g., to forbid infinite scrolling or to demand algorithms to be less addictive) require heavy-handed oversight, and are likely to fail in the long run, as incentives remain to circumvent the rules. Examples of weak compliance and circumvention of existing rules show already prominently under the current regulatory framework. This prominently

includes weak implementations of age verification, which can easily be circumvented by minors (Bursztyn et al., 2026; Fegert & Melchior, 2026; Internet Matters, 2026) but also patchy and weak implementations and effects of screen control settings, or parental control settings (Fegert & Melchior, 2026; Internet Matters, 2026; Stoilova, Bulger & Livingstone, 2024).

Therefore, in this report, we do not attempt to map service features to risks in order to inform policymakers which features are risky for children and hence need to be regulated. This has been done in other reports, such as the “Online Minor Protection Matrix” (Manolios et al., 2026), which links prominent service features like “beauty filters” and “loot boxes” to the above-mentioned 5-C risk typology, and which is prominently featured in the report by the Special Panel on Child safety Online (Fegert & Melchior, 2026, p. 71). Instead, we explain **such service design features as outcomes or manifestations of the rational business logic that ultimately strives to maximise profits**. At the heart of profit maximisation lies the maximisation of revenues, which is the product of demand times price. We argue that firms are willing to employ potentially harmful features in their services, if these have a measurable positive effect on demand or price. In order to be comprehensive, we thereby construe “demand” and “price” widely. The “price” refers to the monetisation channel of the service, which can be collected on the side of the user of the service directly (such as through a subscription or one-off payment) or from another, interlinked market side, such as payments from advertisers. “Demand” refers to more usage of the service, which can be monetised directly or indirectly, such as a higher number of unique users, more frequent use by the same users, or more user engagement and time spent online (which enables, e.g., the service to show more ads).

For example, a social networking service (SNS) would provide “beauty filters”, which are known to create mental health issues and low self-esteem in users (Garg et al., 2026), to enable users to easily create professional-looking, aesthetically pleasing user-generated content, which tends to increase user engagement (Li & Xie, 2020; Ibanez-Sanchez et al., 2022). More engagement, in turn, is associated with more time spent online by users (Allcott et al., 2020; Aridor et al., 2024), which expands the SNS's advertising inventory and hence its revenues (Anderson & Coate, 2005; Anderson & Jullien, 2015; Prat & Valletti, 2022). Further, loot boxes, i.e., lotteries that offer random rewards to be used in games, which are linked to compulsive and addictive behaviours (Brooks & Clark, 2019; Fegert & Melchior, 2026, p. 69) have been shown to induce overspending and increase willingness-to-pay (Cordes, Dertwinkel-Kalt & Werner, 2024; Dertwinkel-Kalt et al., 2025), thus stimulating revenue generation by enabling the firm to sell the game rewards at a higher price.

Conversely, we posit that curtailing those profit maximisation incentives that are linked to creating risks for children online will lead to a rebalancing of corporate incentives, whereby incentives to protect children online regain weight relative to pure profit maximisation – levelling the scale depicted. We believe this ultimately induces rational firms to develop safer and more responsibly designed online services, without the need for a heavy-handed regulation of specific features, functionalities, and formats that is likely to be complex and costly and yet ineffective, as features can evolve quickly and intentionally to evade enforcement. This shortcoming of a feature-based regulation is also highlighted in the report by the Co-Chairs of the Special Panel on Child Safety Online (Fegert & Melchior, 2026, pp. 100-101). Aligning safety with the economic architecture of the business model, like we propose, by contrast, creates a self-sustaining, structurally secure environment.

3.2.A Framework to Connect Business Models to Risk

Against this backdrop, **we propose a framework that links the 5C risk categories to business model characteristics. The framework is agnostic of existing legal categorisations and specific design features**, such as “beauty filters” or loot boxes, and instead forms associations between the risks and demand-enhancing or monetisation enhancing features of the business model. In order not to confuse these features with design features, we refer to the demand-enhancing or monetisation enhancing features of the business model as “dimensions”. The framework assesses to which degree the service providers’ revenue generation depends on these problematic dimensions of the business model.

We identify a total of **seven business model dimensions** that we link to the five risk categories. These dimensions, which we explain in more detail below, assess the impact on the revenue generation of a business.

- (1) Revenue impact of *usage duration* (related to Consumer Risk)
- (2) Revenue impact of *opaque monetisation strategies* (related to Consumer Risk)
- (3) Revenue Impact of *availability of harmful content* (related to Content Risk)
- (4) Revenue impact of *content generated by users* (related to Conduct Risk)
- (5) Revenue impact of *inter-user interaction* (related to Contact Risk)
- (6) Revenue impact of *user data collection* (related to Cross-Cutting Risk)
- (7) Revenue impact of the *use of experimental technology* (related to Cross-Cutting Risk)

Abstracting complex online business models into **seven core dimensions is, of course, a simplification** that does not come without trade-offs. On the one hand, the framework should not include too many business-model dimensions in order to enable the applicability of the framework across the large variety of digital services and their heterogeneous business models. In this sense, fewer dimensions should also render the framework more future-proof and applicable to new business models and new types of digital services that are yet to emerge. This would not be the case if the framework were too detailed (i.e., encompassed too many dimensions) and would be retroactively fitted to the business models and digital service categories that are considered particularly risk-inducing today.

On the other hand, at a minimum, each risk category of the OECD framework should at least be set in relation to one business model dimension. The suggested framework maps seven dimensions to five risk categories. For consumer risks and cross-cutting risks, respectively, two dimensions are proposed, as these could not be adequately captured by one dimension alone. In the context of our framework, the consumer risk category is especially important, because it links directly to monetisation strategies by the service provider, and hence financial gains.

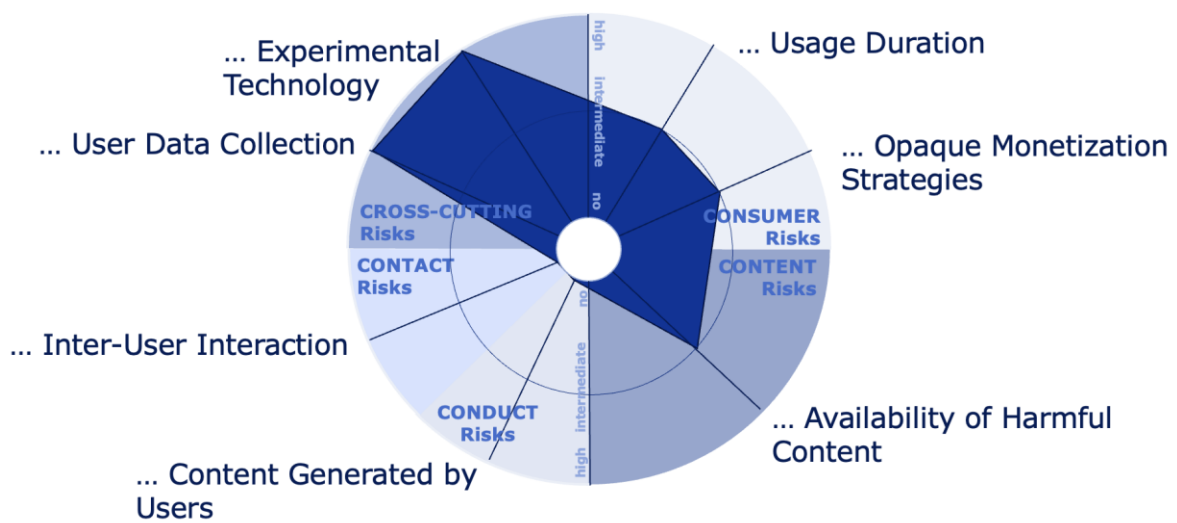
As we will explain in more detail below, a given business model should be assessed along each dimension of the framework with respect to how important that dimension is for the business model’s success, i.e., its contribution to the service provider’s revenue generation. This scoring cannot be done mechanically but requires in itself abstraction and thoughtful deliberation and is thus to some extent dependent on subjective deliberation. To provide a certain level of objective usability, the **scoring of each dimension is in the following operationalised using a three-tiered scale** (no reliance,

intermediate reliance and high reliance). However, the framework is not limited to this three-tiered scale and could also be assessed on a more fine-grained level.

Aligning and arranging the five risk categories and seven business model dimensions on a circle allows for a visual representation of the framework. Scoring an online service's business model in the framework results in a spider-web-like representation of a business model risk profile. In general, the larger the area taken by the spider web, the higher the risks associated with that particular business model. We exemplify and detail the scoring of each dimension in more detail in the subsequent section alongside examples and guidelines when applied to contemporary business models.

*Figure 1: Exemplary application of the proposed framework:
Mapping business models to risk categories on the basis of seven business model dimensions*

Impact of ... on Revenue Generation



3.2.1. Business Model Dimensions Relating to Consumer Risks

Consumer risks are central to our framework, as they relate directly to potential harms that arise from commercialisation. More specifically, we **associate consumer risks with potentially harmful monetisation strategies, i.e., the “price” component in the revenue generation**. We identify two distinct business model dimensions: The reliance of the business model (or revenue generation) on i) usage duration and ii) opaque monetisation strategies. While both target the financial inexperience of users, they stem from different economic drivers for a firm's monetisation design. These two categories reflect the two-fold scaling of commercial interactions online: the frequency with which users encounter them and the transparency with which they are communicated. Naturally, the more time a child spends online, the more advertisements or opportunities for commercial transactions they encounter, be it through direct payments for taking out a subscription, or by watching advertisements and paying with their attention (Engels & Potthoff, 2025; Munzer et al. 2024; Riedel et al. 2025). Therefore, the risk for harm lies at the interrelation of these two forces: Usage duration acts as a multiplier that is set up to maximise a child's exposure to commercial setups, while opaque

monetisation exploits children's developmental vulnerabilities by obscuring the true nature of those transactions (Engels & Potthoff, 2025; Feijoo & Sádaba, 2022; Gath & Swit, 2024; Kumar, Sharma & Agarwal, forthcoming; Munzer et al., 2024). In the following, we explain each of these two consumer-risk-related business model dimensions in more detail.

Impact of Usage Duration on Revenue Generation

This dimension assesses **how much a business can benefit from keeping a user actively engaged on the service, as a means to the end of continuously presenting them with monetisation touchpoints**. Business models that rely on frequent and continuous monetisation-relevant interactions, such as showing ads, provide strong incentives for a service design that purposefully increases the user's time on the service. Prime examples are the endless scrolling mechanism on social networking services, autoplay features on a streaming service or addiction-inducing algorithmic personalisation of content (5Rights Foundation, 2021; Aridor et al., 2024; Beltrán, 2025; Engels & Potthoff, 2025; European Commission, 2024a). These design features, which have been front and centre in the discussion about the protection of minors (Buiten & Busch, 2025; Fegert & Melchior, 2026; Livingstone & Third, 2017; IEEE, 2021), are symptoms of a service provider's incentive to keep users online as long as possible. To assess this dimension, we propose the following guiding question:

How much does the service benefit financially from keeping the user online one more minute?

The question points at a service provider's marginal incentives to prolong a usage session, and links revenue generation directly to the time a user spends online and the frequency of monetisation. In answering this question, we do not strive for a precise quantifiable assessment. We acknowledge that this is challenging, especially without access to business sensitive and firm-privileged data.³ Instead, the idea of our framework, and in answering its core guiding questions, is to **make a qualitative assessment of the business model based on observable characteristics**. In the following, we exemplify the scoring of this, and the following dimensions based on a three-tier qualitative assessment (no, intermediate, high) and provide guidance on which observable dimensions can be used for the assessment.

- ***No impact of usage duration on revenue generation:*** The business's revenue, if any is generated at all, is entirely decoupled from the time a user spends on the service. Prolonged usage duration may even indicate system friction or poor user experience rather than financial gain. This tier would apply to non-commercial websites, utility services like education portals or digital tools.
- ***Intermediate impact of usage duration on revenue generation:*** As soon as the business model can monetise the user, some reliance on the user's duration of service usage is typically created. This reliance may still be low when the service is financed via one-time decisions like signing up for a subscription or upgrading to the premium option of a freemium service. In order to feel compelled to spend money on a service, the user needs to value the service highly enough. The valuation may increase the more time the user spends on the service so that the business might be designed to create habit-like usage patterns to bind users long-

³ At the same time, we do think that a quantifiable assessment could be developed in the long term, especially when privileged information could be acquired by authorities using formal requests for information.

term (5Rights Foundation, 2021; Aridor et al., 2024; Beltrán, 2025; Esposito & Cathoud Ferreira, 2024; Flayelle et al., 2023). In general, we posit that the **longer the interval between usage and monetisation, the more the service provider is aligned with keeping the user satisfied in the long run, and hence less prone to opt for harmful design choices, such as design choices** that spur short-term addictive behaviour (Ichihashi & Kim, 2022) or induce low levels of content moderation (Liu et al., 2022). For example, we deem an annual subscription to a service as generally less prone to creating consumer risks than a short-term, say weekly, subscription period. But, in both cases, and at intermediate impact of usage duration on revenue generation, the usage duration translates into financial gain not immediately but rather in the mid- or long-term through a continued customer relationship, e.g., continued renewal of a subscription to the service.

- **High impact of usage duration on revenue generation:** At this level, the service benefits more immediately from keeping a user online for another minute. This is especially the case for **attention-driven business models that rely on monetisation through advertisements**. Each minute that the user stays online longer enables the business to show more ads, which translates directly into more revenue. This provides the service with the strongest incentives to design the service in such a way that the users are kept engaged and online as long as possible. This means that spurring addictive and compulsive use of the service directly translates into financial gains for the service provider. Next to advertisement-based business models, a high reliance on usage duration can also occur, for example, in **pay-to-win games**, where users are frequently presented with opportunities to purchase game rewards or enhancements that facilitate, or in some cases are required for, continued game play (King & Delfabbro, 2018; Montag et al., 2019).

Impact of Opaque Monetisation Strategies on Revenue Generation

This next dimension, related to consumer risks, examines the **transparency, or rather opaqueness, of the service provider's monetisation mechanics**. In this context, opaqueness refers to the structural covertness of online transactions that are set up to be as frictionless as possible. In many instances, this leads to a service designing its monetisation to intentionally confuse or mislead users. This creates an information asymmetry, leaving underage users in an informational deficit where it becomes increasingly difficult for them to objectively assess how much money, time, or personal data they are “trading” to use the service. For example, in several game apps, providers deliberately obfuscate the relationship to real money by introducing virtual currencies that are designed to detach in-game spending from real-world spending which is shown to alleviate the “pain of paying” (Prelec & Loewenstein, 1998) and can lead to increased expenses (Cordes, Dertwinkel-Kalt & Werner, 2024; Petrovskaya & Zendle, 2022; Raghurir & Srivastava, 2008). In other instances, such as for loot boxes, the price may be communicated clearly, but it is opaque what the value is that the user gets in return. In an advertisement-based business model, it may be difficult for children to discern ads from organic content, and opaque to them how much they are actually “paying” the service with their attention and data. To operationalise the scoring of this dimension, we propose the following guiding question:

How evident is it to the user how they are paying, for how long they are paying, and what they are getting in return?

Structurally, the more a service benefits financially from covert transaction environments, the more intricately those are designed and therefore a higher consumer risk is created. Therefore, for a service whose revenue model depends on frictionless, impulse-driven transactions, introducing total transactional transparency directly works against its financial incentives, leading them to accept financial risks for consumers as a byproduct of their profit maximisation.

In the following, we provide guidance on how to score and evaluate this dimension based again on three levels:

- **No impact of opaque monetisation strategies on revenue generation:** Every transaction, if any, is clearly communicated, e.g., via sticker prices and clear purchase contracts. The user knows at every point in time what and how they are paying and what they are getting in return.
- **Intermediate impact of opaque monetisation strategies on revenue generation:** While the transaction is still clearly communicated, some degree of **operational opacity** is introduced by the service. This could include auto-renewals of subscriptions or hurdles of cancellation. The higher the hurdles of cancellation or the less transparently a renewal is communicated, the higher the service would score on this dimension. Business models that rely on such “dark patterns” seek to exploit user biases and heuristic decision-making mechanisms, e.g., inertia or overestimation bias, to maximise revenues and are quite common among digital services (Beltrán, 2025; Esposito & Cathoud Ferreira, 2024; Busch & Fletcher, 2024; European Commission, 2024b). As was mentioned above, the use of microtransactions with virtual currencies obscures the nature and specifics of the transaction further and alleviates the “pain of paying” (Prelec & Loewenstein, 1998) and can lead to increased expenses (Cordes, Dertwinkel-Kalt & Werner, 2024; Petrovskaya & Zendle, 2022; Raghurir & Srivastava, 2008). This is very common in online video games (Flayelle et al., 2023; Gray et al., 2018; King & Delfabbro, 2018).
- **High impact of opaque monetisation strategies on revenue generation:** In the highest tier, the service provider’s revenue generation is **structurally dependent on informational asymmetry**. Here, monetisation relies to a high degree on masking the true economic cost or true value of the transaction. We argue that this is the case when services are monetised via advertisements, because it is structurally opaque to the user what financial value they are generating for the service in terms of their attention (Bhargava & Velasquez, 2021; Riedel et al., 2025), a vulnerability that is especially pronounced among children who lack the developmental literacy to understand these underlying data-and-attention business models (Fegert & Melchior, 2026; OECD, 2021; O’Neill, 2023). This is further aggravated if advertisements are presented in such a way that it is difficult to discern them from organic content on the service. Another highly opaque monetisation technique especially common in video games is the use of loot boxes, where users buy a ticket to a digital raffle of items without knowing what they will receive in the end (Miao & Jain, 2024; Wardle & Zendle 2021; Zendle et al., 2020). Due to its similarity to gambling and its structural opaqueness of the transaction itself, this also represents a very opaque type of transaction, while also taking advantage of children’s impulse control (Flayelle et al. 2023; Livingstone and Smith, 2014).

3.2.2. *Business Model Dimension Relating to Content Risks*

The third dimension of the business model relates to the content risk by focusing on the **impact of the availability of harmful content on revenue generation**. By “harmful” we denote content that is legal, but not appropriate for children. While the digital ecosystem inherently contains a vast array of any kind of material, a service’s contribution to creating the content risk depends on the extent to which it incorporates and uses harmful content for value creation. Depending on its business model, a service may offer content either as the core value offering or as a secondary feature. This content may either be created first-party by the service (i.e., is fully under its editorial control) or third-party by users. Furthermore, content can be presented in different degrees of vividness, i.e., audiovisual complexity, in the form of symbols, text, songs, pictures or videos (Steuer 1992; Calvert, 2008, OECD, 2021). The probability of experiencing harm from a piece of content is increasing with a higher vividness of the content and repeated exposure to it, as this triggers more intense neurological (and emotional) processing (5Rights Foundation, 2021; Calvert, 2008; Munzer et al. 2024).

In either case, as long as harmful material remains accessible, and its existence is contributing to the commercial success of the service in question, the service providers’ incentives to remove this type of content or to take serious measures to restrict access to it (e.g., through age verification), are not fully aligned with the protection of minors, as any such restriction or removal has a negative financial impact on the service provider. Hence, a risk that children are exposed to harmful content (e.g., because of poor content moderation or ineffective age verification) while using the service is generated (OECD, 2021). To operationalise the scoring of this dimension, we propose the following guiding question:

How much demand would the service lose if they removed all harmful content from the service?

The reduction in demand can be either at the extensive margin (i.e., reduction in the number of users) or the intensive margin (i.e., reduction in the usage intensity): At the extensive margin, demand may be lost by removing harmful content, as users who are expecting sensationalist or taboo content shy away and do not find it anymore; at the intensive margin, users may reduce their usage duration when only less harmful content is available on the service. This is because harmful content, such as misinformation and sensationalist content, is known to grab user’s attention (5Rights Foundation, 2021; Germano, Gómez & Sobbrío, 2026; Milli et al., 2025; Munzer et al. 2024; Ribeiro et al., 2020). In particular, when services pursue an ad-based business model and have an incentive to keep users online as long as possible, recommender algorithms tend to spread engaging harmful content in order to keep users engaged on the service, and consequently the removal of such content would likely have a sizeable effect on the intensive margin of those services.

Next, we exemplify how the hypothetical loss of demand from a removal of harmful content could be qualitatively assessed on a three-tier scale. A higher loss in demand signals a higher impact of harmful content on revenue generation.

- **No impact of harmful content on revenue generation:** The service’s **core architecture precludes the display of expressive content**. It is therefore impossible for harmful or adult-oriented content to exist within that service. There may not be any online service that fits this definition accurately as content even in its basic form is used by almost every online service.

However, basic utility and productivity tools, like a calculator app, could be considered to have no reliance on the existence of harmful content in the service.

- **Intermediate impact of harmful content on revenue generation:** As soon as the service's architecture allows for content to be disseminated, a content risk is potentially created. A loss in demand would then happen, when the content is interwoven into the service offering to a degree such that users expect to find harmful content, i.e., specific demand is created. This could be the case for social networking services that offer a large variety of content to cater to many different user tastes, of which some seek harmful content specifically. Also related to social networking services is the function of harmful content as an attention driver. Many content algorithms may use sensationalist, i.e., sometimes harmful content to keep users engaged and curious to prolong their usage duration (5Rights Foundation, 2021; Aridor et al., 2024; Munzer et al. 2024). If this is possible, then the impact of harmful content on revenue generation is increasing as such attention-keeping mechanisms unconsciously influence demand of users for more content by getting them hooked and potentially also creating demand out of habits or even addiction (5Rights Foundation, 2021; Aridor et al. 2024; Beltrán, 2025; Esposito & Cathoud Ferreira, 2024; Flayelle et al., 2023).
- **High impact of harmful content on revenue generation:** The highest demand loss after the removal of harmful content will be experienced by **services for which the dissemination of harmful content presents the main value proposition**. This applies, e.g., to adult content websites or conspiracy theory websites. Since the majority, if not all of the content these services offer is harmful to children according to our definition, removal of that content would inevitably lead to an almost complete loss in demand for those services.

3.2.3. *Business Model Dimension relating to Conduct Risks*

The fourth structural pillar of our framework assesses the conduct risk dimension, which we link to **the impact user-generated content (UGC) has on revenue generation**. While the previous dimension assessed the availability of harmful content in general, irrespective of how and by whom it was created, in this dimension we focus on the ability of users of a service to create and disseminate content directly. As the conduct risk is created through children's own actions online, a channel through which these actions can take place is required; and hence the conduct risk can be tied to the possibility to disseminate content on the service themselves. Prototypical examples of user-generated content are videos and pictures that are disseminated by a social networking service, but our conceptualisation also includes other forms of content, originating from users, rather than the service itself, such as comments and likes. More generally, UGC can be of varying degrees of vividness, as already defined above, among others, symbols, text, songs, pictures or videos (OECD, 2021, Steuer, 1992). Even UGC with low vividness, such as likes and dislikes, can cause harm to children, e.g., through negative impacts of such externalised feedback on self-esteem during age periods with a heightened sense for external approval (Fegert & Melchior 2026, p 39). In reverse, in the hope of receiving comments and likes, children may also be incentivised to produce more harmful content themselves, exacerbating the conduct risk. Given that UGC is the primary channel through which conduct risks can

be facilitated, we propose the following guiding question to tie UGC to the business model of a service provider:

How much demand would the service lose if it disallowed user-generated content?

For some business models, allowing user-generated content may be integral to their demand creation and value proposition either at the core or as an additional feature. Social networking services, for example, operate as “empty vessel” that offers the foundational structure for dissemination of UGC, but rely almost exclusively on users to populate the network with content and interactions (Aridor et al., 2024). Therefore, social networking services have an incentive to design the service in such a way that participation and creation of content are frictionless in order to maximise content on the service – and with it ultimately demand and revenues. Giving users such media-vivid tools for self-expression directly amplify the possibilities to not only participate as a contributor but also as an aggressor, creating a profound conduct risk (O’Neill, 2023). But since these content-based interactions are integral to providing value and network effects for the service, and therefore also for revenue maximisation, restricting a user’s ability to participate and to create content directly disrupts the value proposition of the service, creating a tension between mitigation of conduct risks and profit maximisation (Aridor et al., 2024; Engels & Potthoff, 2025).

The qualitative assessment of a service’s economic reliance on user-generated content can be guided as follows:

- ***No impact of UGC on revenue generation:*** The service does **not allow any user-generated content**. All available content is first-party content, i.e., provided or commissioned by the service itself. Hence, users can only consume content, but not disseminate any content of their own, including comments that can be seen by others. This would apply, e.g., to many streaming services without comment functions that only host own or licensed professional content.
- ***Intermediate impact of UGC on revenue generation:*** If a commercial service allows for UGC, it is safe to assume that it does so in expectation of raising its demand and revenues; hence the removal of UGC is likely to have a negative impact on the demand and revenue generation. However, the **degree to which UGC is relevant for demand generation can vary significantly across services**. For example, consider an online video streaming service, or an online dictionary, which hosts only first-party curated content, but allows users to comment on the content, e.g., providing opinions on the movies, or adding their own translations. In this case, the business model reliance on UGC is low, i.e., the removal of UGC would only have a small negative impact on the demand and revenue generation of that service. Clearly, the more integral UGC is for the service’s value proposition, the higher is the impact it has on revenue generation.
- ***High impact of UGC on revenue generation:*** The highest level of impact is reached when a **service almost exclusively disseminates UGC**, like social networking services or online discussion websites. This means that the service only provides the technical infrastructure that enables the creation and sharing of content by users but does not provide a significant amount

of content itself. For these services, often the quantity rather than the quality of user contributions is a priority, which translates to ample opportunities to use the service-given tools and infrastructure with malicious intent for example, cyberbullying or sharing misinformation (Aridor et al., 2024). Here, UGC is the main value proposition of the service, and thus the creation and dissemination of content is usually made as frictionless and media vivid as possible (5Rights Foundation, 2021). Without UGC, the services' value proposition collapses, and an almost complete loss in demand would follow (Aridor et al., 2024, 5Rights Foundation, 2021).

3.2.4. *Business Model Dimension relating to Contact Risks*

The fifth business model dimension of our framework is the **service's systemic reliance on inter-user interaction**, which we associate with the contact risk. While the previous dimension isolated the creation and dissemination of (harmful) content as a means to communicate, in this dimension we focus on the nature of interaction. As soon as a service implements a feature that permits lateral communication between two or more users, at least one of them being a minor, the possibility for a contact risk is created (OECD, 2021). The reliance of a service provider's business model on inter-user interaction may differ greatly. A messenger service, for example, creates its value for users entirely from facilitating direct or group interactions, whereas an online game may implement a chat function between players as an additional feature (Sas & van der Hof, 2025). Following our above definition of content, any kind of symbol, text, song, picture or video (Steuer, 1992; Calvert, 2008) through which communication is facilitated is considered content that can potentially be harmful and using higher-vivid content will increase the risk for harm (5Rights Foundation, 2021; Munzer et al. 2024).

While conduct risk is created by minors as the senders of harmful content, contact risk is created when minors are the recipients of harmful content, including content sent by adults. Receiving content from other people depends on the reach of interaction between users; for example, how easily a stranger can initiate contact in public community conversations or send a child a private message. Services whose main value proposition is to facilitate direct communication between users have fewer incentives to restrict reachability of their users and hence are more incentivised to design communication as frictionless and far-reaching as possible, while significantly increasing the contact risk simultaneously (Aridor et al., 2024). Therefore, we assess this dimension with the following guiding question:

How much demand would the service lose if it restricted inter-user interaction?

The qualitative assessment of a service's reliance on inter-user interaction can then be guided by the following categorisation:

- ***No impact of inter-user interaction on revenue generation:*** The service does not have any technical infrastructure for inter-user interaction and **operates entirely without any features for social interaction**. This would often apply, e.g., to productivity tools including services like AI assistants. This could also apply to services that provide content, e.g., a streaming service, but that do not allow users to interact with each other.
- ***Intermediate impact of inter-user interaction on revenue generation:*** Whenever a service

allows any form of inter-user communication, it does so to enhance its value proposition, and hence the demand for its service. In reverse, restricting inter-user interaction again after it has become part of the service's revenue generation would have a negative impact on demand. For **many service providers inter-user communication does not constitute the main value proposition and is merely an ancillary feature of their service.**

An online commerce platform, for example, might also offer a chat function for direct interaction between buyers and sellers, which facilitates the matching of supply and demand on the platform, but is not strictly dependent on it, as is also the case in an online game with a chat function that is still playable without the communication feature (Sas & van der Hof, 2025). Consequently, removing this feature would not make the service itself useless but would still mean that some users that relied on this chat function to be more informed about their purchases, or to communicate with their friends, might opt for another service. Additionally, in many games, inter-user interaction is a more central feature of the value proposition. Allowing gamers to interact with each other contributes significantly to the value and enjoyment created by the service. Yet, many games would remain playable, even though less enjoyable, and therefore less demanded, if inter-user interaction was restricted. Also, many social networking services allow for direct inter-user interaction, such as through direct messages, and comments and public community replies to posts. While this creates an important part of the social networking service experience, there arguably may still remain demand if direct user interaction is restricted and only user-generated content remains accessible, especially by those users that only seek to passively consume content (Aridor et al., 2024; Valkenburg, van Driel & Beyens, 2022; Verduyn, Gugushvili & Kross, 2022).

- **High impact of inter-user interaction on revenue generation:** If a service's **main value proposition lies in connecting users and facilitating communication**, restricting this communication would deprive the service of its identity and would not provide any substantial value to its users anymore with a detrimental impact on the demand of that service. This would clearly be the case for messenger services that are built to connect users.

3.2.5. Business Model Dimension relating to Cross-Cutting Risks

With respect to cross-cutting risks, which are meant to capture any risks not addressed in any of the other risk categories, we propose to focus on two business model dimensions that seem particularly relevant in the context of online services. The first dimension is the impact of user data collection on revenue generation, which links commercial incentives to cross-cutting risks, more specifically privacy risks. The second dimension is the impact of experimental technology on revenue generation, which is primarily meant to link risks associated with the use of AI to business models that are reliant on the provision and use of AI tools.

Impact of User Data Collection on Revenue Generation

Continuously collecting vast amounts of personal user data allows services to refine and personalise

their content algorithms and also serve highly targeted advertisements to increase the service provider's overall profitability, such as to leverage demand through personalisation, increase the effectiveness of targeted advertisement or to decrease the cost of innovation (Flayelle et al. 2023; Johnson, Shriver & Du, 2020). Especially when the service in question is part of a larger firm ecosystem, user data can be used to leverage these advantages also into related service markets, (Boyer, 2022; Flayelle et al. 2023; Krämer & Schnurr 2022; Krämer & Shekhar 2025).

This critical reliance of digital business models is starkly demonstrated by the consequences of previously implemented regulatory interventions that restrict user tracking and personalisation. For instance, when policy interventions prohibit behavioural profiling and personalised advertising on content specifically targeted at kids – like it was the case after a ruling of the COPPA (Children's Online Privacy Protection Act) in the US – the loss of high-impact targeted ads can result in immediate, severe revenue drops for the service (Johnson et al., forthcoming). This revenue deficit can trigger a direct “privacy-for-content” trade-off: Decreasing the impact of data-driven revenue generation, content creators have been shown to reduce content supply as well as quality and originality (Johnson et al., forthcoming), which immediately affects the monetisation potential of the service as a whole.

A service's financial model can depend so heavily on this data feedback loop that any restriction would cost it revenue and value. This creates a powerful incentive for the provider to intensify data collection and user tracking instead. This may also translate into the design of the service's choice architecture for collecting consent for such data collection via e.g., opt-in prompts. The guiding question for this dimension is therefore:

How much can the service benefit financially from collecting and using personal data in its ecosystem?

Assessing this dimension is difficult, as the level of data collection and how data is used to increase profitability is often opaque outside the firm. Nevertheless, we believe that a qualitative assessment can be made, for which we provide some guidance in the following discussion:

- ***No impact of user data collection on revenue generation:*** The service does **not collect or store any user data**, and therefore cannot profile and track users, nor use personal data for commercial monetisation. We recognise that there are few services that would fall under this ideal, but it presents a useful theoretical case nevertheless.
- ***Intermediate impact of user data collection on revenue generation:*** As argued above, user data can be used in various ways by firms to enhance revenue, and many services are able to collect such data as a byproduct of the usage of their service (Goldfarb & Tucker, 2019; Krämer & Schnurr, 2022). Therefore, service providers will often collect personal data, at which point the collection has a structural impact on revenue generation of a firm. The degree to which user data collection impacts revenue generation will vary greatly across services. One can roughly distinguish **two dimensions along which online service providers accumulate user data**: The breadth of a data set, i.e., the extent to which it represents the full user base, and its depth, i.e., the length and granularity of the profile held on each individual user (Krämer &

Schnurr, 2022).

Data collection and analysis along both dimensions translate into financial gains, albeit through different mechanisms:

- Increases in breadth improve the accuracy of aggregate models such as demand forecasts, search rankings, or ad-targeting algorithms (Krämer & Schnurr, 2022; Schaefer & Sapi, 2023; Aridor, Che & Salz, 2023; Klein et al., 2022), but exhibit positive yet diminishing returns, as each additional user adds progressively less new information once the data set is already broadly representative (Krämer & Schnurr, 2022; de Fortuny, Martens & Provost, 2013; Bajari et al. 2019).
- Increases in depth, by contrast, sharpen personalisation for the individual user and generate a positive externality on predictions for other, similar users, which is the underlying source of data-driven network effects that further enhance the value of the service and hence demand (Prüfer & Schottmüller, 2021; Bergemann, Bonatti & Gan, 2022; Yoganarasimhan, 2020).

Thus, it is fair to assume that the more user data a firm collects, and **the more the service is prone to personalisation, the more it benefits financially from user data collection**. For example, this relates to services that rely in their demand generation and value proposition on personalised content feed or recommender systems.

- **High impact of user data collection on revenue generation:** A high impact of user data collection can be assumed when a **service cannot only use personal data to improve its service quality**, which then has an indirect positive impact on financial gain in the long term, but when personal data can be translated into a positive financial gain more immediately. This is typically the case when a firm's revenue generation depends predominantly on targeted advertisements. Through data collection, the accuracy of targeting, and hence the effectiveness of advertisement can be improved, which immediately translates into financial gains (Johnson, Shriver & Du, 2020). Note that this scoring also depends on the nature of advertising. In our assessment, a firm that only pursues contextual advertising, for which it is not necessary to build extensive user profiles, scores lower than a firm that relies on targeted advertisements and for which it needs to build user profiles.

Further, **because breadth and depth are complementary and can be expanded at low marginal cost by providers that already operate at scale**, dominant incumbents and service providers that operate an ecosystem of services, as opposed to a single service, and cross-use data between those services, are able to convert their user data advantage better into higher service quality, more effective monetisation of advertising inventory, and superior revenue, while simultaneously raising the entry barriers faced by competitors that lack comparably broad and deep data resources (Krämer and Schnurr, 2022; Schaefer & Sapi, 2023; Klein et al. 2022). Thus, large dominant providers, such as

gatekeepers under the DMA, and providers with an ecosystem of data-intensive services tend to score high in this business model dimension.

Impact of Experimental Technology on Revenue Generation

The seventh and final dimension of our framework evaluates the generation of cross-cutting risks by assessing the **importance of experimental technology for a service's revenue generation**. While we draw on the foundational conceptualisation of automated and data-driven systems encompassing among others AI and predictive analytics by the OECD (2021), we intentionally deviate from the OECD's original wording of "advanced technology" and call our dimension "experimental technology". We do so in favour of a more focused approach that better captures the unpredictability and unproven risk potential of technology. Additionally, by posing the term "experimental technology" we are able to provide a more neutral and future-proof framing.

With our approach to this dimension, we mirror Fegert and Melchior's (2026) approach. For them, the core logic for risk stemming from technology is rooted in the ever-evolving environment around digital services that makes the risk potential of new technology nearly impossible to anticipate. **The newer and untested a technology is, the higher the structural risk from potentially harmful outputs that will only become visible once** a technology is deployed and its behaviour is made observable (Fegert & Melchior, 2026). Today's prime example of this is generative AI or similar black-box machine learning algorithms. As soon as a service integrates these technologies to deliver its core value proposition, experimental technologies become impactful for a service's revenue generation. The extent to which this technology is integrated into the core value proposition is important for its overall impact. For example, embedding generative AI features into a service is becoming more and more widespread, either to enhance a service (e.g., to facilitate the creation of social networking service posts) or as the main feature of the service itself, as in the case of AI assistants.

This increasing integration of AI features into online services poses significant risks for children's well-being. For example, excessive AI use, especially of social chatbots, can lead to psychological dependence (Phang et al., 2025; Xie, Pentina, & Hancock, 2023; Yu, Chen & Yang, 2024), especially for children and for people with mental health problems (Hu, Mao & Kim, 2023; Huang et al., 2024; Yu, Chen & Yang, 2024). These attachments can go as far as to be ranked as equal to human interaction or even replace real-life social interaction (De Freitas et al., 2025; Laestadius et al., 2024). It is also reported that people with mental health concerns that turn to AI assistants as emotional support were reinforced by the chatbots to engage in harmful and abusive behaviour (De Freitas & Cohen, 2025), further solidifying the harmful direction such technology can guide users to. Evidently, the more centrally generative AI is embedded in and tied to a service's value proposition and revenue generation capabilities, the more willing the services risks associated with the use of that technology is the service provider willing to accept.

Therefore, we pose the guiding question for this dimension:

How much does the service benefit financially from using experimental technology?

We stress that the relevant question is not unpredictability from the use of experimental technology as such, but unpredictability that the firm has a financial stake in. We propose the following guideline for the assessment of a service's reliance on experimental technology:

- **No impact of experimental technology on revenue generation:** In principle, every digital service inherently operates on a baseline level of technical risk, as any hardware or software employed may not work as intended due to human error, technical failure or malicious external actors. However, we deem services that do not rely on self-learning algorithms, therefore **delivering predictable outcomes**, e.g., through lookup in a database as in the case of an online dictionary, or simply relay messages to and from users without algorithmic curation, as having low impact of experimental technology on a service's revenue generation.
- **Intermediate impact of experimental technology on revenue generation:** Assessing the structural unpredictability of technology is difficult, as digital risks frequently only materialise aftermarket launch as features interact in unpredictable ways (Fegert & Melchior, 2026). For this first guideline we suggest the differentiation based on the output of the technology. If an entirely new real-time output can be synthesised, i.e., an output that can by definition not be anticipated prior to generation like it is the case with generative AI (Fegert & Melchior, 2026), we categorise the service under the highest category. Any other technology scores in this middle category which means that any output, while being unanticipated, needs to be a known item.
- **High impact of experimental technology on revenue generation:** The **business revenue generation relies on systems characterised by deep structural unpredictability**. Instead of serving a known item, the engine is able to synthesise entirely new real-time outputs in any form. The behavioural boundaries of such systems remain largely unmapped and can exhibit unpredictable behaviour not anticipated by the developers. But if by using these technologies a substantial amount of revenue can be generated, incentives are high for the firm to use it regardless of its unintended consequences. This would for example apply to generative AI assistants. They are a fairly new phenomenon of the last three years and are at this point in time prone to function in ways unintended by the user as well as the developer.

4. Putting the Framework to Use

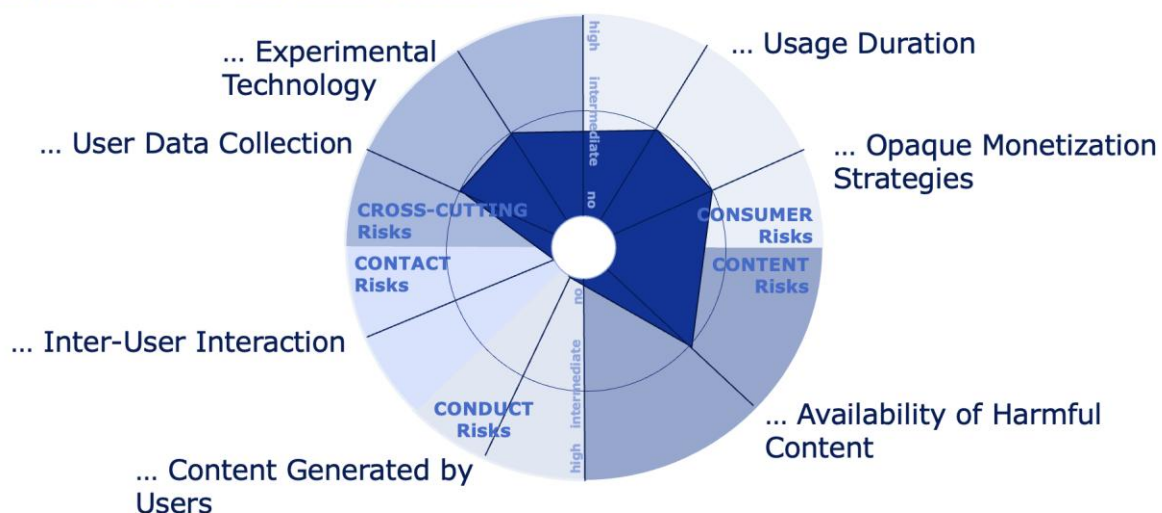
To validate the operational utility of our framework, this section applies our scoring criteria to three prototypical digital business models:

- A subscription-financed video streaming service providing predominantly first-party content;
- an advertisement-financed social networking service, relying predominantly on user-generated content,
- and a subscription-financed AI assistant, that responds to queries by users using generative AI.

4.1. Subscription-financed video streaming service with predominantly first-party content

Figure 2: Exemplary scoring of a subscription-financed video streaming service with predominantly first-party content

Impact of ... on Revenue Generation



The scoring is based on the following rationale:

- Usage Duration: Intermediate – Revenue is generated via a flat subscription fee rather than per-impression ad views
- Opaque Monetisation: Intermediate – Prices and contracts are transparent, though auto-renewals introduce minor operational opacity.
- Harmful Content: Intermediate – A video streaming service usually has some content inappropriate for children but does not rely entirely on such content for profit generation.
- User-Generated Content: No – The service hosts exclusively first-party or licensed professional content. Users cannot upload media.
- Inter-User Interaction: No – No direct messaging, public chat, or social networking features exist between users.
- User Data Collection: Intermediate – Usage data is collected to power recommender algorithms and personalisation, but data is typically limited to viewing history.

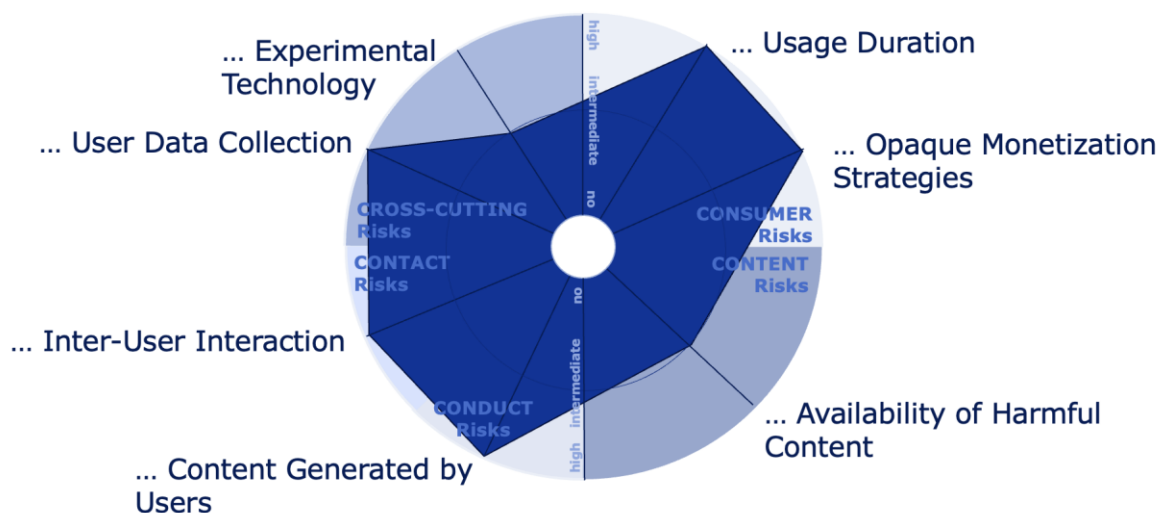
- Experimental Technology: Intermediate - Uses machine learning for recommendations, but outputs are strictly bounded to a catalogue of known items.

Overall assessment: The service does not score high in any of the seven dimensions. Business incentives that may create harm arise mainly from the availability of potentially harmful content (e.g., age-inappropriate movies) and the collection and use of personalised data to fuel recommendations. Notably, if the service were to adopt an ad-financed business model, partly or in full, the risk profile would increase, as the impact of usage duration on the service's revenue generation becomes more pronounced.

4.2. Ad-financed social networking service

Figure 3: Exemplary scoring of an advertisement-financed social networking service

Impact of ... on Revenue Generation



The scoring is based on the following rationale:

- Usage Duration: High – as the service is ad-financed, keeping users engaged and online allows the service to show more ads and to collect more data to improve ad targeting and personalisation of content.
- Opaque Monetisation: High - The revenue generation is “hidden” behind a free service that monetises via ads and data collection mostly unnoticed for the user.
- Harmful Content: Intermediate – The service has among other content harmful content available to be used to draw attention to optimise session duration.
- User-Generated Content: High – The service relies highly on high vividness user-generated content to populate its value proposition.
- Inter-User Interaction: High – The service enables multidirectional communication via text and with unmoderated media. Unassociated people can message each other.
- User Data Collection: High – The business monetises user data and benefits highly from intricate user profiles through better targeting and personalisation of content feeds.

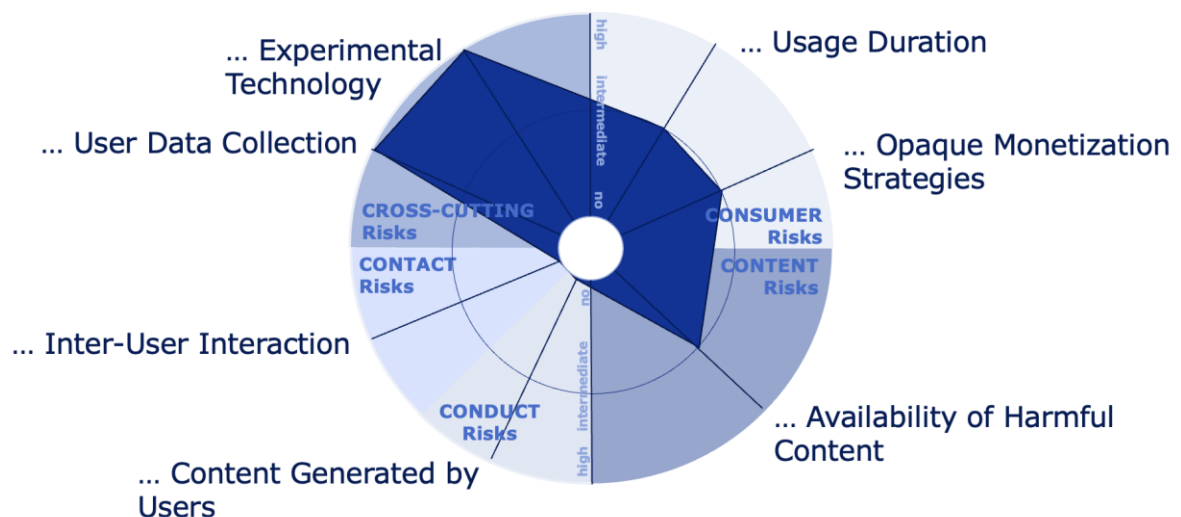
- **Experimental Technology:** Intermediate – The service depends on recommendation algorithms that self-optimize without direct oversight, but outputs are strictly bounded to a catalogue of known items.

Overall assessment: A prototypical social networking service creates a **high-risk profile** in the proposed framework, due to its reliance on advertisements, which provides incentives to keep children online as long as possible, and the reliance on user-generated content, and inter-user interaction. Business incentives to create and tolerate a risky online environment for children are thus particularly high in this business model, also in comparison to other digital business models assessed in this section.

4.3. Subscription-financed AI assistant

Figure 4: Exemplary scoring of a subscription-financed generative AI service

Impact of ... on Revenue Generation



The scoring is based on the following rationale:

- **Usage Duration:** Intermediate – The service operates task-driven and provides a timely defined utility to the user. The evaluation would change to “high” if the generative AI service is monetised through an ad-based business model as then financial incentives to induce longer usage duration are greater, which could potentially lead to greater health consequences, as higher daily usage is also associated with higher perceived AI dependence among children (Robayo-Pinzon et al., 2025).
- **Opaque Monetisation:** Intermediate – The monetisation utilises a hybrid freemium model with nudges to upgrade to a subscription with more utility. Additionally, auto-renewals introduce minor operational opacity.
- **Harmful Content:** Intermediate – The service relies on providing unfiltered output to meet adult users’ expectations, creating a continuous risk of exposing children to harmful content as well. Misinformation and disinformation are also possible.
- **User-Generated Content:** No – The service does not disseminate user-generated content in a way that can create a conduct risk, although the service’s output is also based on content that

is available online, including user-generated content.

- Inter-User Interaction: No – The service does not facilitate interactions between users.
- User Data Collection: High – The service needs to collect high amounts of user data and keeps extensive memory of those to personalise the user experience.
- Experimental Technology: High - The service uses generative AI technology that can lead to unpredictable outcomes.

Overall assessment: The risk profile of AI assistants is predominantly shaped by their use of experimental technology, which can lead to unpredictable outcomes and can (re-)produce harmful content. Depending on its use, the service potentially also collects large amounts of personal data. The use of AI assistants bears significant operational costs for the provider, which limit its incentives to keep the users online as long as possible. However, **this evaluation changes significantly** if the AI assistant were to pursue an ad-financed business model. This would create higher incentives to collect and exploit personal data and to keep the users engaged.

4.4. Intermediate Conclusions

Three conclusions follow from the analysis so far.

First, **different business models generate different risk profiles for children**, as the preceding examples illustrate. The structure of a firm's monetisation strategy and the nature of its core value proposition determine which risk categories are more likely to emerge and which are suppressed. In particular, whether a service is **subscription-based or ad-based matters for the risk profile**, even if it would often not matter for the legal characterisation of such services.⁴ The magnitude of financial return derived from risk-inducing design choices is inversely related to the incentive to mitigate the corresponding risks: the greater the revenue that a firm extracts from such structures, the higher its tolerance for the risks they entail, and the weaker its incentive to reduce them.

Second, this heterogeneity has direct implications for regulatory design. Business models differ systematically not only in the severity of the risks they produce but also in the number of risk dimensions they implicate. **Regulatory stringency should therefore be calibrated to risk severity**, with more restrictive obligations applied to business models that generate more severe or more numerous risks. The framework developed in this report provides a first comparative basis for identifying which business models, and which specific dimensions within them, warrant priority regulatory attention. While the resulting recommendations do not necessarily entail an outright ban, in some cases restricting children's access to a given service may be the appropriate measure.

Third, the **risk-inducing dimensions of the business model are often interrelated and reinforce each other**. Take consumer risk and content risk for example. As was explained, sensationalist, and therefore oftentimes harmful, content is used in social media algorithms to prolong the usage duration to achieve higher financial gains through advertisements. Keeping users on the service longer also increases the possibilities for data collection which becomes more intrusive the more the service is

⁴ For example, the legal definition of an “online social networking services” under the Digital Markets Act (DMA), Art. 2.j.7 is not dependent on how the service is monetised, and states that it is “a platform that enables end users to connect and communicate with each other, share content and discover other users and content across multiple devices and, in particular, via chats, posts, videos and recommendations”. Likewise, none of the definitions of the services in scope of the Digital Services Act (DSA), Art. 3 refer to their business model and monetisation strategy.

able to monetise this data. Taken together, this business model scores high on at least three risk dimensions because of this interrelation. Therefore, we can also conclude that risk dimensions seldom exist in isolation but most often facilitate each other and arise together in very interwoven structures.

5. Service Access Layers and Service Ecosystems

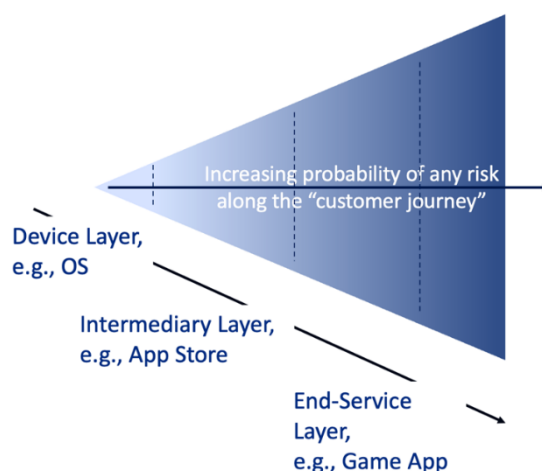
The framework developed so far considered a given service, operated by a single provider. However, digital services are often nested: in order to discover, access or use one service, a user usually has to pass through one or several other services first. A game is found and installed through an app store, which in turn runs on an operating system; or a website is reached through a browser and typically found through a search engine. What may appear, from the child's perspective, to be the use of a single service is in fact the use of a stack of services, each with its own provider, its own business model and, by the logic of our framework, its own risk profile.

Figure 6 visualises this **layered structure of online access, using the example of three layers**:

- A *hardware/OS layer*, relating closely to the device that the child is using and on which services run,
- an *intermediate layer*, denoting platforms that the child may use to discover, display or buy content, such as app stores, browsers or search engines;
- and the **end-service layer**. Consider a child playing an online game on a smartphone.

The operating system makes the installation of applications possible in the first place. The OS is usually not monetised directly but financed through the price of the phone or a licence agreement. The app store is often the intermediary service through which the game is discovered and downloaded and through which its in-app purchases are processed; it is typically financed by sponsored placement and a commission on the revenue the game generates. The game itself may monetise through various means such as discussed previously, including advertising, loot boxes or other in-game transactions facilitated through virtual currencies or in-app purchases. Therefore, **each of the three providers pursues its own revenue-maximising logic**, and each therefore inherits a distinct risk profile along the seven dimensions of our framework, varying both in severity and in the number of dimensions implicated.

Figure 5: Visualisation of Layered Online Access



5.1.1. Risks tend to accumulate along the service layers

Because every layer contributes a profile of its own, **the risks to which a child is exposed when using a nested service accumulate. This accumulation operates through three channels.** First, exposure is additive: For example, the operating system collects device-level data that may be shared within the ecosystem of the provider; the app store monetises through promoted placements and opaque in-app purchase flows, and the game adds usage-duration incentives, loot boxes and inter-user interaction on top of both. The child's aggregate exposure is the union of the profiles of all services in the stack, not the profile of the end-service alone.

Second, the upstream layers act as gatekeepers: what a child can reach at all is determined by which applications an app store admits and which results a search engine surfaces, so that a permissive upstream layer transmits and multiplies the risks created downstream.

Third, the layers are financially interlocked, and their incentives therefore presuppose one another. Because an app store earns a share of the revenue an application generates, it also has an incentive to look the other way and to maintain availability and access to a service, even where the monetisation technique in question, loot boxes being the clearest example, is precisely the kind of design our framework identifies as risk-inducing. Risks at different layers thus reinforce each other rather than arising independently.

5.1.2. Misaligned incentives tend to be stronger at the end-service layer

At the same time, and this is our second observation, the **possible conflict between profit maximisation and the protection of children is not of constant intensity across layers. It weakens systematically with distance from the end-service.** At the end-service layer the relationship with the user is immediate, and so is monetisation: Each of the risk-inducing dimensions of our framework translates more or less directly into revenue at this layer, and every safety measure that introduces friction translates just as directly into revenue forgone.

One layer up, the relationship becomes indirect. An app store earns a standard commission on transactions, typically between 15 per cent and 30 per cent (Google, 2026; Apple, 2026), but it does not earn the advertising revenue that an individual application generates from a marginal minute of use, and its own value proposition also rests on the perceived quality and trustworthiness of the catalogue as a whole rather than on the success of any single application within it. Its incentives are therefore generally better aligned with protecting children online.

At the device layer the relationship is more indirect still. An operating system provider monetises the installed base and the overall attractiveness and stability of its ecosystem, and it therefore derives the least direct financial benefit of all three layers from any specific risk-inducing design choice. Its risk profile is not merely different in shape from that of an end-service; it is likely to span a smaller area in total.

5.1.3. Economic incentives to properly exercise control functions for child protection, such as age verification, are best aligned at the device layer

Taken together, the previous two observations yield the following insight: the **misalignment of incentives that our framework identifies as the root cause of online harms is least severe at precisely those layers that are technically best placed to mediate access**. Safety functions that require a service to turn users away, age assurance above all, but also default restrictions on data collection, purchasing or contact, are most credibly exercised by a party that does not lose money by turning them away. Two qualifications are in order. First, the argument is comparative rather than absolute: intermediary and device layer providers are not disinterested parties, and wherever they operate end-services or advertising businesses of their own, the conflict reappears within the same firm. Second, under current market conditions the two dominant mobile operating systems are owned by the same firms that operate the dominant app stores, so that the device and intermediary layers are in practice partially merged and the commission revenue of the store accrues to the same entity. This complicates the attribution of financial reliance to particular layers, but it does not overturn the underlying logic: even a vertically integrated provider of an operating system and an app store earns far less at the margin from one child's extended session in one application than the operator of that application does.

Where an end-service is required to verify the age of its users, it bears the cost twice over: the direct cost of operating the check, and the indirect but far larger cost of the users, and the usage duration, that the friction of verification removes from its monetisation pool, not only for children but also for adult users as all users have to be subjected to age verification. The more robust the check, the greater the loss. Weak and easily circumvented checks, such as a self-declared date of birth or a simple tick box, are therefore not an implementation failure but the predictable outcome of assigning the task to a party that is financially penalised for performing it well. This is consistent with the widely documented ineffectiveness of age assurance in current practice (Bursztyn, 2026; Fegert & Melchior, 2026; Internet Matters, 2026).

Locating age verification at the device layer significantly reduces this conflict. An operating system provider does not depend on the user volume or the usage duration of any individual application, and it is technically positioned to establish a verified age signal once, at the point of entry into the digital environment, and to make that signal available to every intermediary and end-service above it. A single robust check at the device layer also spares the child from repeating an identity-revealing verification at every service they use, which sits more comfortably with the principle of data minimisation than the per-service approach that currently prevails; the tokenised, double-blind architecture envisaged in the European Commission's April 2026 recommendation is well suited to being anchored at this layer. The app store constitutes an alternative and a useful complement, since it is the point at which an application is actually obtained and at which age-appropriate distribution can be enforced, and since it too is relatively insulated from the monetisation of any single application. However, we do acknowledge that placing age verification at the device or intermediary layer could further entrench existing gatekeeper positions.

We also recognise that there are practical questions of accountability and cost distribution that would

need to be addressed and resolved when demanding that one commercial entity (the operating system or app store provider) operating at a lower service layer conducts the age assurance for another commercial entity – even if they are to some degree already interwoven, and commercially co-dependent on each other, as they operate in the same digital (mobile) ecosystem. We will return to this point when we make our recommendations on age verification in Section 7.3.

What the layered perspective argues definitively against is the current default, under which responsibility for age verification rests with precisely the actor whose business model gives it the strongest reason to under-deliver on it. This does not absolve end-services of their responsibility for age-appropriate design; it does suggest that the verification of age itself belongs further down the stack, or to a completely independent neutral third-party, where the check does not compete with the revenue of the party performing it.

6. EU Digital Rulebook

6.1. Current rulebook

In the following, we lay out the general EU legal framework on the protection of minors, its problems and highlight the reforms that are planned by the European Commission (Buiten, Ledger & Busch, 2025; Busch, Fletcher & Ledger, 2026; Ledger, 2026). Details of the current rules and options for future reforms are presented in the recommendations section.

The current framework is complex, yet the rules are of a general nature. The complexity stems from the fact that the **framework is mainly composed of rules that apply to certain services, which are characterised in the legal texts by reference to what these services aim to achieve, rather than by reference to their business models and their underlying risk profiles**. Only a few rules are horizontal in nature meaning that they apply to all service providers, but again irrespective of the business model. The rules are also rather general leaving Member States the freedom to enact more far-reaching rules for some pieces of legislation or leaving the service providers the ability to decide how to protect minors.

Historically, the **first set of EU-level rules to protect minors was contained in the Television Without Frontiers Directive** and aimed to protect minors (and viewers in general) when they were watching television. Rules have since been added to also protect minors when they watch on-demand audiovisual content that is curated by a video streaming service provider such as Netflix or Prime Video. Some rules were also added to the Audiovisual Media Services Directive (AVMSD) in 2018 to protect minors⁵ when they watch user generated videos on video sharing platforms (VSPs) such as YouTube.

One of the key characteristics of the rules to protect minors that stem from the AVMSD is that they allow the Member States to introduce more far-reaching rules to protect viewers. The Member States have very much used this possibility for linear and non-linear services but not so much in relation to the protection of minors on VSPs. The other key element to note is that the AVMSD's rules to protect minors follow a **tiered approach**: more rules on the protection of viewers in general (and hence minors also) when they watch TV, (slightly) fewer rules when watching on-demand services and less detailed rules to protect viewers and minors when on VSPs. The logic is fair: when there is editorial responsibility of service providers (i.e., they choose the programmes in the schedule or the catalogue), they are in control and can protect viewers and minors. For VSPs the logic is different, content is uploaded by others, and they do not have editorial responsibility over the content that is uploaded by users.

On top of this, the Digital Services Act (DSA)⁶ carries over the e-Commerce Directive's⁷ **no general monitoring obligation**. According to this principle, intermediary services cannot be subject to a general obligation to monitor the information they transmit or store, or to a general obligation to actively seek facts or circumstances indicating illegal activity which includes social media platforms (but not providers with editorial control). This is important to keep in mind when devising rules to

⁵ Art.28b AVMSD.

⁶ Art. 8 DSA.

⁷ Art. 15 Directive 2000/31/EC.

protect minors online.

The **DSA** is the other main piece of sector-specific legislation that contains rules to protect minors online. The main articles of interest are:

- Article 28 (1) DSA according to which online platforms (such as social media, video-sharing platforms, app stores and marketplaces - but not online search engines and not online platforms that qualify as small and microenterprises) that are accessible to minors must take appropriate and proportionate measures to ensure a **high level of privacy, safety, and security of minors**. The European Commission has issued guidelines (which are used by competent authorities as a benchmark to assess compliance) to help online platforms comply with this part of Article 28 (European Commission, 2025a).
- Article 28 (2) DSA provides that online platforms **cannot present advertisements based on profiling** (as defined in the GDPR) by using the personal data of minors (to the extent that they are aware, with reasonable certainty, that they are minors).
- Articles 34 and 35 whereby the online platforms (and search engines) designated by the European Commission as very large (active monthly EU users above 45m) must **annually assess negative effects of their services for the protection of minors**, the rights of the child, and serious negative consequences for their physical and mental well-being and mitigate any identified systemic risk. The list of possible mitigation measures they need to deploy includes age verification, parental control tools and tools to help minors signal abuse or to obtain support. The European Commission has announced on multiple occasions that it is prioritising the enforcement of the rules on the protection of minors of the DSA.

A key characteristic of the DSA is that it is a regulation, meaning that it is directly applicable in the Member States' legal order and it does not allow them to set additional obligations on intermediary service providers.

The only horizontal rules are contained in the **General Data Protection Regulation (GDPR⁸)** and in the **Unfair Commercial Practices Directive (UCPD)⁹**.

- Article 8 GDPR provides that when data processing is based on consent¹⁰ and when online services are directly offered to children, the processing is lawful where the child is at least 16 years old. If the **child is below 16 years, consent should be given** or authorised by the holder of parental responsibility. However, the Member States may set a lower age for when children can begin to give consent, if it is not below the age of 13.
- The UCPD prohibits misleading or aggressive practices that could materially distort the economic behaviour of an average consumer. Article 5(3) UCPD recognises that **children are 'vulnerable consumers'** but does not attach a direct consequence to that fact, for instance by stating that traders need to be particularly mindful of not exploiting their vulnerability. Instead, the article states that commercial practices that are likely to materially distort the

⁸ Regulation (EU) 2016/679.

⁹ Directive 2005/29/EC.

¹⁰ In many cases, data controllers opt for other legal basis than consent to process the personal data of minors, such as the execution of a contract or legitimate interest (Galissaire, 2025)

economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, need to be assessed from the perspective of the average member of that group. The UCPD also refers to the concept of targeted average consumer. If a commercial practice targets a certain group of consumers, then the practice needs to be evaluated from the average member of that specific group.

On top of the complexity of the rules, the current legal framework presents **other problems**.

- The rules do **not always lead to a change in the business incentives** of the online services that are causing harm to children. They often have few incentives to comply with some of the rules, and this is creating enforcement difficulties.
- The rules have so far **not led to a level playing field**. Some services (hardware and operating system providers, e-commerce websites, video gaming platforms, gambling websites, porn services, AI assistants, etc.) may only be covered by horizontal rules, even though they may carry risks to minors, albeit the risks are different depending on the service.
- Many Member States are seeking to introduce social media bans because the **Member States are concerned that minors are far too exposed** to harmful and illegal content online. These national laws are most often not in line with the country-of-origin principle of the E-commerce Directive or with the full harmonisation approach of the DSA¹¹. This is therefore creating internal market fragmentation. The French Constitutional Court has also ruled that the French social media ban is contrary to the constitution of France on the grounds that it is not appropriate, necessary and proportionate to the objective pursued (Conseil Constitutionnel, 2026).

The **Artificial Intelligence Act (AI Act)** also contains specific rules that are relevant for the protection of minors.¹² Article 5(1)(a) prohibits the use of an AI system that deploys purposefully manipulative techniques that materially and harmfully distort people's decision-making behaviour. Article 5(1)(b) extends this to include AI that **exploits certain specific vulnerabilities**, including age, to materially and harmfully distort behaviour. The European Commission has recently adopted guidelines on the AI Act that list, for instance, that Article 5(1)(b) could cover *"A game uses AI to analyse children's individual behaviour and preferences on the basis of which it creates personalised and unpredictable rewards through addictive reinforcement schedules and dopamine-like loops to encourage excessive play and compulsive usage"* (Para 105). It must also be noted that these rules have not yet been tested. Further, the rapidly evolving nature of AI technology has already led the European Commission to propose a Digital Omnibus on AI to introduce more rules to protect minors. In particular, AI systems that generate non-consensual, sexually explicit and intimate content or child sexual abuse material (like nudification apps) will be prohibited.

Gen AI models also need to undergo specific **risk-management processes** and deployers will need to report to the European Commission on the results of this process before models are made available on the market. Specific transparency obligations apply since August 2025 to make sure that people

¹¹ Art. 3 Directive 2000/31/EC.

¹² Regulation (EU) 2024/1689.

are aware that they are interacting with an AI system, instead of a human and to inform when content has been artificially generated or manipulated.

6.2. Outlook

In terms of outlook, following the publication of the Special Panel's¹³ recommendations (Fegert & Melchior, 2026) on 13 July 2026, the **EU Kids Act** was proposed by the European Commission on 17 September 2026. It covers social media services and VSPs, which are subject to the strictest rules, as well as AI chatbots and companions, app stores and video gaming (platforms and services). It contains age restrictions to access social media and VSPs, whereby for social media and VSPs:

- below the age of 13, children should not get access. By way of derogation, they could access specifically designed VSP services through their guardian's account (under conditions);
- between 13 and 15, children could access these services through 'mini accounts' (with limited features) supervised by guardians;
- Between 15 and 18, children could access services through their own accounts, provided the services comply with safety by design obligations, addressing addictive design, unwanted contacts, unsafe settings and recommender systems.

These age restrictions would only apply where a social media service or a VSP poses a risk to privacy, safety or security of a minor below 15. According to the European Commission, this is presumed to be the case when the service comprises at least one of the five functionalities listed in the proposal (such as addictive design features or recommender system based on profiling).

The proposal contains safety-by-default rules which vary according to the type of service, and which apply for users below the age of 18. The strictest rules apply to social media and VSPs and largely build on the Article 28 DSA guidelines. AI chatbots and companions and online games would be subject respectively to different tiers of obligations.

On oversight, the EU Kids Act proposal largely relies on existing enforcement structures under the DSA and the AI Act. The data protection authorities would also have enforcement powers to ensure that data protection principles under the GDPR are respected in relation to age verification. The proposal has been portrayed by the European Commission as reversing the burden of proof. The two main mechanisms foreseen are:

- that services that need to comply with safety-by-design rules could only derogate from these rules once they have established that users are above 18 by using an age assurance measure;
- social media and VSPs that are also VLOPs under the DSA would be obliged to submit a compliance plan (where they demonstrate compliance with rules) to the European Commission within 30 days from the entry into force of the regulation (4 months from designation for newly designated VLOPs). Compliance plans would have to be audited by independent auditors with specific expertise.

¹³ In September 2025, the president of the European Commission, Ursula von der Leyen, announced the setting-up of a special panel of experts to develop a "strong and practical European approach to keep children safe online."

The European Commission is also set to publish a proposed **Digital Fairness Act (DFA)** at the end of 2026, which is expected to tackle unethical techniques and commercial practices related to dark patterns, marketing by social media influencers, the addictive design of digital products and online profiling, especially when consumer vulnerabilities are exploited for commercial purposes.¹⁴ The DFA will be horizontal legislation and is framed as a consumer law instrument. It is also intended to have a particular focus on the protection of minors.

The **AVMSD** is also under review and a proposal to amend that framework is also expected to be adopted before the end of 2027. The European Commission will need to evaluate the DSA by 17 November 2027 and possibly propose reforms to the regulation.¹⁵

Ideas to adapt the legal framework to address harmful business models are presented below.

¹⁴ President of the European Commission, Mission Letter to Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection Michael McGrath, 1 December 2024, p. 7.

¹⁵ Art. 91 DSA.

7. Policy Recommendations

Building upon our proposed framework, in the following we will outline some policy recommendations designed to align the economic incentives of actors within the digital ecosystem with the protection of children online. We first derive these recommendations directly from our preceding analysis and insights while remaining largely agnostic of the existing legal framework in the EU. Subsequently, we contrast these proposed interventions with the current EU regulations to evaluate what is already adequately addressed and to pinpoint critical regulatory gaps. Before detailing these specific recommendations, however, the following subsection provides a foundational overview of the legal framework to date, examining current mechanisms and identifying potential issues within its application.

7.1. General Framework

Recommendation 1: (Risk-based oversight)

Regulation should scale with the risk a service's business model creates for children. Because risk-inducing elements of a business model reinforce one another and jointly shape a provider's financial incentives, oversight should tighten in step with a service's overall risk profile and user base — up to and including restrictions on how, or whether, that business model may serve children.

Against the backdrop of the preceding analysis, our primary overarching recommendation is that regulatory oversight must scale with the risks a service's business model creates for children. Our framework provides a systematic assessment of a service's risk profile rooted in observable business model characteristics and the firm's economic incentives. When a service's risk profile is low, its economic objectives are substantially better aligned with the protection of children than when its risk profile is high. Because these risk-inducing elements often reinforce one another to jointly shape a provider's financial incentives, regulatory oversight should tighten with the overall risk profile up to restrictions and bans. By focusing on these underlying economic drivers, our framework remains intentionally agnostic to existing legal classifications of service types, such as those recognised under the DSA or the AVMSD. Yet, many of these services that tend to score highest within our risk assessment, such as social networking services, are already subjected to some regulation under these existing frameworks.

In particular, given the current political debate to ban the use of social networking services for very young users in the EU (Fegert & Melchior, 2026), this shows that the framework has **diagnostic value in identifying problematic business models**. However, our framework is meant as the starting point of a debate that links harms for children more systematically to financial motives of online service providers, and a tool that structures this debate along the seven dimensions proposed. In its current state, it does not yet lend itself to determining a precise quantitative threshold at which a service ought to be considered “high-risk”, and we acknowledge that the appropriate classification as a “high risk” service warrants more detailed research.

We have exemplified our framework through a qualitative assessment of each dimension, using three tiers (no, intermediate, high), but the application is not limited to these three tiers. **In our three-tier framework, to fix ideas and to set a starting point for the discussion, we propose to consider a service overall “high-risk” if it scores “high” on at least three dimensions.**

Future research should develop more quantitative and analytical approaches to assessing each dimension; for example, in a similar vein to how the hypothetical monopolist test was developed as an analytical test under competition law for determination of the ‘relevant market’ and ultimately ‘market power’ (OECD 2012), two legal concepts that are per se qualitative and not quantitative in nature.¹⁶ We argue that a similar toolset could be developed to assess the hypothetical impact on revenues for a given service in any of the seven dimensions in our framework. Until then, we argue that also a qualitative risk assessment is feasible, and, as we show next, not unprecedented under current EU law.

Indeed, **current EU-level legislation integrates to a certain extent, albeit in an incomplete manner, the idea that the more a service carries a risk the more it should be regulated.** The DSA and the AI Act are probably the legal instruments that embody this idea the most. The DSA contains most of the rules on the protection of minors online as explained above. It considers that the more reach a service has, the more it should be regulated. On the protection of minors, this also means that intermediary services that are not online platforms, very large (i.e., that reach at least 45m monthly active users in the EU) online platforms or search engines, do not need under the DSA to protect minors online, even if a service is very risky. Also, if an online platform qualifies as a small or micro enterprise, it does not need to protect minors even if its business model has a high-risk profile. VLOPs and VLOSEs have more obligations than online platforms that do not reach the thresholds. This shows that the DSA considers that the risk profile of a service is dependent on its reach and not on the underlying risk profile of the business model, although the wording of Article 28 of the DSA is so general that this cannot be ruled out either as an approach.

Zooming out further, beyond the DSA, **some services are not subject to any rules, beyond horizontal rules.** This is the case for hardware/OS providers, e-commerce websites, video gaming platforms, gambling websites, porn services with no user-generated content, or AI assistants that could not be considered as intermediary services. Although it is clear that not all of these services carry risks for minors, this situation has created some legal gaps that the European Commission is seeking to fill in the upcoming reforms of the Digital Fairness Act (DFA) and of a legal instrument to ensure the protection of minors online. The Special Panel has also recommended that AI companions, gaming companies and other digital services should be covered by future legislation (it refers to social media+) which shows that the DSA’s scope of application is in some respects too narrow to ensure the protection of minors online (Fegert & Melchior, 2026).

This report therefore argues that new legislation is needed on the protection of minors online. In an **effort of simplification of the existing legislative framework, this new legislation should replace other sector-specific rules** and in particular Article 28 of the DSA. (European Commission, 2025b). This legislation should in part be **designed according to the risk profile of business models rather than**

¹⁶ Specifically, the hypothetical monopolist test considers whether a firm, if it were the only firm in that market (a hypothetical monopolist) could profitably undertake a small, but significant and non-transitory increase in price (SSNIP), typically 5 per cent. If this is not the case, then the relevant market is considered too wide, and must be construed more narrowly until the hypothetical monopolist test is met.

based on service categories that may not fit all business models, and may not be future-proof, as service characteristics tend to change quickly and soon services may not fall squarely under these legal definitions anymore. This represents a leap forward in legal thinking but seems a logical approach for three reasons:

- It targets the root cause of the harm rather than the symptom. As explained above, this means for instance that instead of prohibiting infinite scrolling for minors, which is a design feature intended to keep minors online as much as possible because of an advertisement-based business model, emphasis is placed on restricting the ability to present advertisements to children;
- It moves away from a service centric approach, which as we have shown presents weaknesses. Not all services have the same business model whereas they are regulated in the same way: Wikipedia is for instance regulated under the DSA as a VLOP, whereas it is not funded by advertising but from donations and avoids advertising. Some gaming platforms do not present characteristics of intermediary services under the DSA whereas they may present risks to minors (and adults) (Sas & van der Hof, 2025).
- It is likely to be much more future proof. As discussed below, emerging services such as AI assistants already illustrate that new digital services do not always fall neatly within existing service-centric regulatory frameworks, whereas business models are generally more stable and may therefore provide a more robust basis for classification.

Building a model around the risk profiles of business models is likely to be more future proof, but new legislation on the protection of minors should also be inherently flexible to address emerging phenomena. We therefore recommend that legislation is **supplemented by legally binding standards that could be easily adapted over time, possibly through delegated or implementing acts**. Strong oversight is also needed to ensure correct implementation.

The experience of implementing the DSA also shows that the protection of minors may require a more prescriptive regulatory approach. Rather than relying on broad, principle-based obligations and ex post enforcement, legislation should impose clear ex ante rules and prohibitions. Children should not remain exposed to potentially harmful content and practices while the European Commission carries out lengthy investigations, adopts infringement decisions, which are often challenged before EU courts.

The proposed framework for mapping business models to risks provides immediate insights into which dimensions of a business model prompt risk, and which restrictions placed on the business model could mitigate that risk. For example, restricting and regulating more tightly how and whether service providers can pursue an advertisement-based business model would rebalance incentives to keep the user online, and hence reduce the service provider's risk profile in our framework. In the following section, we propose a set of seven targeted recommendations, one for each dimension in our framework, on restrictions that could be placed on a business model with the goal of reducing the risk profile of the service. **Because risks tend to be interrelated, and the dimensions on the business model tend to reinforce each other, combining different targeted recommendations would be more effective than just the sum of its parts.**

We argue that such a targeted approach, especially for high-risk services (cp. Recommendation 1) would also be **more proportionate and likely more effective than an outright ban of the service for children**. An outright ban often sparks the desire in children to circumvent the restriction and to use the service nevertheless – which then is likely to be even less safe. Furthermore, our recommendation of targeted interventions that address the incentives of the service provider to create a risky environment would allow for a developmental approach, whereby the restrictions could be differentiated by age of the users and gradually lifted as the child matures and gets acquainted with the risky online environment. This developmental approach aligns directly with that proposed by the Report of the Co-Chairs of the Special Panel on Child Safety Online (Fegert & Melchior, 2026). Against the backdrop of the current EU legal framework, we acknowledge that this approach will however require a change of paradigm from a regulatory/legal perspective. Indeed, as shown above, the current legislative framework is either horizontal or sector-specific, it can be risk-based; but so far it has not been explicitly built around addressing the business models that have been identified as generating risky behaviour.

7.2. Rules Applicable to All Services, Irrespective of Their Overall Risk Profile

In accordance with our overarching Recommendation 1 we suggest a set of targeted interventions along the seven business model dimensions that should predominantly apply to “high-risk” services. However, we also suggest that the dimensions relating to **consumer risks**, that are the business incentives to keep children online as long as possible, and the business incentives to pursue opaque monetisation strategies, as well as **cross-cutting risks arising from incentives to monetise and collect data about children**, should be curtailed for all services, irrespective of their overall risk-profile. This is because these dimensions relate more directly to financial gains of the service provider than the other dimensions. The economic mechanisms underlying these dimensions therefore are most immediately tied to creating a risky environment for children.

For example, if a service does not monetise its users at all, neither through payments from the users directly (e.g., subscriptions) nor through third parties which are provided access to the user’s attention or data (e.g., advertisers) then the service has no financial incentives to expose children to harm. This is not to say that a free-to-all service that hosts harmful content is not also creating a risk to children, but such a service has no economic mechanism (no “price”) to translate that harm into a financial gain; and thus, we argue, that the incentives of such a service are better aligned with the protection of children, for example, by applying effective age assurance measures.

Recommendation 2 (Usage duration)

No service should have incentives to keep children online as long as possible. Therefore, strict advertising limitations should apply for children: Not only with respect to the targeting of advertisements, but also with respect to quantitative limits and qualitative standards for advertisements. For very young children no advertisements should be allowed at all.

Advertising limits can be gradually lifted as the child user matures.

Especially advertisement-based business models create strong incentives to keep users online as long as possible, as discussed above. While a ban on targeted advertisements curtails incentives to collect data, it does not properly curtail the incentives to keep children online as long as possible. To achieve this, **regulation should explicitly target the volume of advertising** such as the number of advertisements that can be shown to children within a day or per session.

Furthermore, for very young children, the incentive to keep the child online should be minimised entirely, which, in our opinion, can only be achieved by **disallowing advertisement-based monetisation** completely. In line with a developmental approach, these strict advertising limits can then be gradually lifted as the child user matures.

Current legal framework

Current EU legislation integrates quantitative and qualitative limits on advertising, and it protects minors from targeted advertising. These limitations, however, only apply to certain services and do not constitute a ban on advertising for minors.

The AVMSD contains advertising **time limits** (quantitative limits¹⁷) that protect all viewers (adults and minors alike) against excessive advertising **on linear television**. (i.e., where there is editorial responsibility). A two-tier cap of maximum **20 per cent applies**: first, between 6am and 6pm, and between 6pm and 12pm. There is no limit on the amount of advertising between 12pm and 6am. Isolated advertising spots are only possible in sports events. The AVMSD also contains additional rules to ensure that certain programs are not interrupted excessively by advertising: children's programs, in particular that they can only be interrupted by advertising if they are longer than 30 minutes, and only every 30 minutes.

The AVMSD also contains **qualitative standards**¹⁸: advertising cannot contain subliminal techniques; damage human dignity; include or promote discrimination based on sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation; encourage behaviour that could be damaging to health or public safety; encourage behaviour that would be grossly damaging to the environment; promote cigarettes (includes electronic cigarettes and refill containers); promote medicines or treatment that is available on prescription (in the country where the service is established).

The directive also contains **additional rules to protect minors against commercial communications that could harm** them morally, physically, and mentally. Commercial communications cannot directly encourage minors to purchase goods or services by exploiting their inexperience or credulity, persuade someone else to buy the advertised product or service or exploit the trust minors place in their parents, teachers or other people. Also, minors cannot be shown in dangerous situations in advertisements. Advertisements of alcohol products cannot encourage immoderate consumption, depict minors consuming alcohol, link consumption to driving, enhanced physical performances, or social/sexual success, claim that alcohol has therapeutic qualities, emphasise high alcoholic content

¹⁷ Arts. 20 and 23 AVMSD.

¹⁸ Art. 9 AVMSD.

as being positive. Also, advertisements for alcoholic drinks cannot be aimed specifically at minors.

Further, audiovisual media services are encouraged to use co-regulation and to foster self-regulation through codes of conduct on inappropriate commercial communications for food and beverages high in sugar, salt and fat in/around children's programs.¹⁹

All these qualitative standards apply to linear TV, on-demand audiovisual services and to video service providers (VSPs) for the advertising that they “market, sell or arrange”²⁰. For other advertising that is not arranged by them, VSPs need to take measures to ensure that those that provide advertising comply with these standards for instance, through their terms and conditions. Member States are free to set more far-reaching rules on advertising in their national legislation.

The **DSA** also contains rules on advertising. Article 28 provides that online platforms must not present targeted advertising to minors.²¹ No other outright advertising ban exists under EU legislation to protect minors online.

Recommendations

Placing limits on the amount of advertising exists under EU law and similar restrictions could be extended to all digital services that have an economic incentive to keep minors online. Limits could be gradually lifted provided the qualitative limits on advertising similar to those of the AVMSD are extended to protect minors online. For example, the following age-dependent advertisement limits seem reasonable to us.

Very young users should not be exposed to advertising at all. This should apply irrespective of the service categorisation and business model. In practical terms, this would mean that all advertisement-funded services would need to introduce some age assurance measure in order to adapt advertisement volume and content accordingly. However, only high-risk services would potentially need to involve a neutral third-party for age verification (see Recommendation 5).

Adolescents can be progressively exposed to advertising, provided quantitative limits apply, irrespective of the service categorisation and of the business model. These limits could be inspired by those of the AVMSD but would need to be adapted to digital viewing habits since daily limits would probably not make sense. All online services, irrespective of their service categorisation and business model, should abide by qualitative standards of protection for adolescents. We see no logical reason why minors should be exposed to advertising that could present a risk to their moral, physical and mental development. We therefore propose that the qualitative rules on advertising of the AVMSD should apply. Last, no minors should be exposed to targeted advertising (as envisaged in the DSA).

Recommendation 3 (Opacity of monetisation)

The service has to provide information to the user on how it is monetised. No opaque monetisation strategies should be allowed for children. This includes clear transparency about advertising and sponsored content,

¹⁹ Art. 6a AVMSD.

²⁰ Art. 28b (2) AVMSD.

²¹ Art. 28.2 DSA specifies that they cannot present advertising based on profiling as defined by article 4 GDPR using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.

clearly marked final prices and fixed contract lengths, and restrictions on virtual currencies as well as probability-based monetisation schemes.

As established in our previous discussion on consumer risks, the structural covertness of online transactions inherently creates an information asymmetry for vulnerable users. When monetisation mechanics are designed to be as frictionless as possible, they often intentionally mislead underage users where it becomes increasingly difficult to objectively assess the true cost – whether in money, time, or personal data – they are trading to use the service. Because service providers structurally benefit from this opacity, thereby accepting consumer risk to be a byproduct of profit maximisation, regulatory intervention is critical to realign this incentive structure. Therefore, no opaque monetisation strategies should be allowed for children, and transparent sticker prices with fixed contract lengths should become the standard.

In particular, this recommendation entails several practical restrictions. First, as far as advertisements are permitted for young users at all, they must be **clearly identifiable** and cannot be embedded in social media feeds or appear like organic content, aligning with principles already established in the DSA and the AVMSD. Second, **probability-based monetisation schemes**, such as loot boxes, should **not be allowed** for children due to their structural opaqueness, similarity to gambling, and exploitation of impulse control, an area anticipated to be addressed under DFA. Finally, the use of **virtual currencies** that explicitly detach in-game spending from real-world financial consequences, alongside intermediate opaque mechanisms like auto-renewing subscriptions that rely on dark patterns, must be **strictly restricted** for underage users.

Current legal framework

There is currently under EU law no obligation for digital services to provide information to the public about how they monetise their service. This **transparency obligation** with sufficient detail to allow for public scrutiny and understanding of the relative importance of each **monetisation strategy** could be added into upcoming EU-level legislation (in particular the **DFA**) similarly to requirements contained in the e-Commerce Directive on the general information that needs to be provided by information society services that need to be made available to recipients of services.²²

There are *transparency obligations at EU level on advertising, but rules are not specific to minors*: Article 26 of the **DSA** provides that online platforms need to ensure that for each advertisement presented, each individual recipient is able to clearly identify that the information is an advertisement (which must be marked as such), the person or organisation on whose behalf the advertisement is presented (and who paid for it, if it is different from the one that presented it) and the main parameters used to determine the recipient to whom the advertisement is presented and how to change these parameters where possible. The article also foresees that online platforms should provide a functionality to allow users to declare if the content they upload contains an advertisement and, in that case, the online platform needs to ensure that recipients of the service can identify that the content is advertising. VLOPs and VLOSEs also need to put in place an online repository containing defined information on all the advertising that has been presented. This allows public scrutiny and

²² Art. 5 of the e-Commerce Directive specifies that at least the following information needs to be made available: name; geographic address of establishment; contact details; supervisory authority; the trade register for regulated professions; the registration body/authority, details for regulated professions, VAT identification number, clear indication of price.

regulatory oversight of their advertising practices.²³

The **e-Commerce Directive** contains an identification requirement for advertising that applies to information society services.

The **Political Advertising Regulation (PAR)** also contains detailed transparency obligations that apply to providers of political advertising services (those that prepare, place, promote, publish, deliver and disseminate political advertising).²⁴ It also prevents the targeting and the use of ad delivery techniques by relying on the use of personal data of minors (defined as one year before the age of voting as defined in national law), when the service provider knows with reasonable certainty that the data subject is a minor (as defined)²⁵.

Loot boxes and probability-based monetisation are not yet clearly regulated under EU legislation, although some of these practices could potentially be restricted under the **Unfair Commercial Practices Directive**. Also, self-regulation has addressed such practices. In particular, the gaming industry abides by PEGI (the Pan European Game Information System²⁶) which requires upfront clarity about loot boxes.

Recommendations

The European Commission's **upcoming proposal for a DFA** will most probably address some of these practices. Commissioner Michael McGrath has publicly said that the European Commission is examining gaming features such as virtual currencies, in-app purchases, gambling-like mechanisms and loot boxes. Possible measures range from warning labels and transparency requirements to parental controls, default safety settings or bans on certain features.

As noted in a previous CERRE report (Busch, Fletcher & Ledger, 2026), it is probably disproportionate for risk-based regulation to simply prohibit these specific design features for all users and in all circumstances because they can bring benefits or are valuable to foster positive engagement. However, **because of the specific vulnerability of minors, we argue that full price transparency for services targeted at or used by minors should be embedded in horizontal EU-level legislation**, such as in the upcoming DFA.

- Current EU legislation governing digital subscription contracts is fragmented which has led some Member States to introduce specific rules on subscription contracts (Busch, Fletcher & Ledger, 2026). The EU-level rules that are relevant for this report to **digital contracting** are contained in (horizontal) consumer protection law and in the DSA. Transparency requirements regarding the duration of the contract and the conditions for terminating are set out in the Consumer Rights Directive (CRD), whereas the CRD, the UCPD and the European Commission's guidance on the UCPD have sought to introduce easier cancellation functionalities for digital contracts.
- Article 25 of the DSA prohibits online platforms from manipulating users or otherwise distorting their ability to make free and informed decisions, including by making it more

²³ Art.39 DSA and recital 95.

²⁴ Regulation (EU) 2024/900.

²⁵ Art. 18.2 Political Advertising Regulation.

²⁶ <https://pegi.info/pegi-code-of-conduct>.

difficult to terminate a service than subscribing to it.

Numerous options are already on the table in the context of the upcoming DFA to provide more protection for consumers (including minors therefore) who are finding it difficult to cancel contracts online, are faced with unexpected auto-renewals or who suddenly find that a free trial has been converted into a paid subscription. These options range from introducing an easy cancellation facility for consumers, the possibility to terminate a contract that has been automatically renewed at any time with a short notice, reminders before subscriptions are automatically renewed or the need for consumers to actively accept renewals.

If these elements are included in the upcoming DFA, we think this would also provide sufficient protection for minors, and we therefore in the spirit of simplification, do not propose that these elements should also be added into specific legislation on the protection of minors.

The general transparency requirement on the monetisation strategy, which is not yet on the agenda of the European Commission could be added to specific legislation on the protection of minors, but we also see that such rules could be beneficial in a wider context so could be added to horizontal legislation such as the upcoming DFA.

Recommendation 4 (data collection)

Collection of personal data of children should be restricted, without the service giving the possibility to consent to more extensive data collection. Restrictions can be gradually lifted as the child matures (e.g., with respect to the type and amount of data collected, and to what extent data can be shared between services operated by the same provider and/or with third parties).

A service provider's structural reliance on user data collection creates a fundamental tension with the protection of minors. Generally, the more personal data is collected, the better it allows the service to refine personalisation algorithms and spur data-driven network effects, thereby increasing demand, or to monetise the data directly, such as through improved targeting of advertising. Particularly providers with a large user base, and providers with several interconnected services operating service ecosystems, benefit from data collection and data cross-use; thus they possess the strongest economic incentives to collect and exploit personal data.

To address this misalignment of economic incentives and user privacy and safety, the collection of personal data of children must be strictly restricted and minimised. **Specifically, we propose that services are not allowed to prompt minors or their legal guardians to consent to more extensive data collection than what is strictly necessary to fulfil the service.** These restrictions can be gradually lifted as the child matures. Collecting data strictly to enhance the user experience of a child should become more and more possible while any use for commercial intent like targeted advertising should stay prohibited for minors.

This recommendation ties in with Article 28 of the DSA which specifies that online platforms need to

ensure a high level of **privacy**, safety and security of minors.

Current legal framework

The EU's legislative framework is quite rich when it comes to protecting the personal data of EU citizens and minors in particular. However, it does not prohibit the collection and further processing of personal data of minors.

As noted above, the **GDPR** contains a special rule on the age of consent. Beyond this, when legitimate interest is relied on to process a child's personal data, the controller needs to make sure that the legitimate interest is not overridden by the interest of the child or fundamental rights. Recital 38 of the GDPR recognises that children merit special protection, especially in the context of using personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

Other sector-specific rules apply to protect minors from platforms wanting to further process personal data of minors that is collected or otherwise generated to protect them (e.g., on age verification or to put in place parental control systems) for commercial purposes such as direct marketing, profiling and behavioural targeted advertising. These rules exist for VSPs (under the **AVMSD**²⁷) and for online platforms (under the **DSA**²⁸).

Also, as seen above, online platforms cannot serve targeted advertising to minors when they are aware with reasonable certainty that the recipient of the service is a minor.

Turning to Article 28 of the **DSA**, the guidelines specify how platforms should ensure the protection of personal data when they deploy functionalities aimed to protect minors such as age verification (e.g., data minimisation principle) or when they use recommender systems (in particular, if a recommender system relies on the processing of behavioural data about a minor, prioritisation should “not rely on the processing of behavioural personal data that is so extensive as to capture all or most of the minors’ activity on the platform”).

Recommendations

For all services and regardless of the business model, we recommend that service providers should be prohibited from further processing the personal data of minors that has been collected to protect them for commercial purposes. Also, we propose that services should not be allowed to prompt minors or their legal guardians to consent to more extensive data collection than what is strictly necessary to fulfil the service. Lastly, as developed above, given that the **DSA** already prevents targeted advertising from being addressed to minors, we suggest that this prohibition applies to all services. Some of these restrictions could be lifted as the child matures.

7.3. Rules Applicable to High-Risk Services

In line with our overarching Recommendation 1, the following list of targeted interventions should apply only to “high-risk” services, that is those services that exhibit an overall high-risk profile in our

²⁷ Art. 28b AVMSD.

²⁸ Art. 28 para 3 DSA.

framework.

Recommendation 5 (Access to harmful content)

For high-risk services, regular external audits of the service's age verification measures and content moderation should be required. In case of shortcomings the service should be mandated to hand over user age verification and content moderation to a neutral third-party.

As established in our previous discussion on content risk, a service's reliance on harmful content may create a fundamental conflict of interest. When the presence of harmful content contributes to the commercial success of a service, whether by capturing user demand directly or by driving usage through attention-grabbing content algorithms, taking serious measures to moderate content or restrict access through age verification leads to restricted monetisation opportunities for the provider. Under these economic realities, the service provider possesses the strongest financial incentives to look the other way, leaving internal content moderation and strict age verification disincentivised. We posit that, when this misalignment of incentives is particularly pronounced, that is if the service is considered in the "high-risk" category, regular external, independent audits of age verification measures and content moderation practices should be required. In cases where shortcomings are observed in these audits, the service should be mandated to hand over its age verification and/or content moderation responsibilities to a neutral third party.

Audits

We acknowledge that implementing a genuinely "neutral" third-party, be it for the audit itself, or for age verification and content moderation, is non-trivial and introduces an economic agency problem: the third-party can have an incentive to please the service that hired them, undermining their neutrality.

In the context of external audits, such misconduct by ostensibly "neutral" firms is well documented—for instance, in the Enron and WorldCom scandals (Demski, 2003), where the auditing firm was financially compensated by the very companies it was tasked with overseeing. Building on the lessons of the Enron and WorldCom scandals, the Sarbanes-Oxley Act (2002)²⁹ in the US introduced several structural safeguards, including mandatory rotation of the lead and concurring audit partners every five years, a prohibition on auditors providing most non-audit services (e.g., bookkeeping, valuation, or internal audit outsourcing) to the same client, and a requirement that audit committees, rather than management, approve and oversee the auditor relationship (U.S. Securities and Exchange Commission (SEC), 2003). Similar rules exist in the EU.³⁰

Empirical research on non-audit fees has generally found that higher fees paid to auditors for consulting services are associated with reduced audit quality and greater earnings management, consistent with an economic bonding effect (Frankel, Johnson, & Nelson, 2002). However, the evidence on mandatory audit firm rotation is more mixed: while proponents argue that rotation reduces the risk of collusion and complacency over long client relationships, a substantial body of

²⁹ Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745.

³⁰ Regulation No 537/2014; Directive 2006/43/EC and Directive 2014/56/EU.

literature suggests that the costs of rotation, including loss of client-specific knowledge and lower audit quality in the initial years of a new engagement, may outweigh its independence benefits (Cameran, Prencipe, & Trombetta, 2016).

Taken together, this literature suggests that no single mechanism fully resolves the underlying agency problem; rather, independence is approximated through a layered system of firm-level reputational incentives, external regulation, and internal governance oversight. Nevertheless, several important insights and lessons can be learned from the experiences in the financial industry when considering the regulatory regimes for mandatory engagement of external auditors, content moderation and age verification providers in the context of digital services.

Our recommendation that **high-risk services should be audited and thereby provide “proof” that they are safe** is also in line with the recommendations of the Special Panel on Child Safety Online which recognises that the **burden of proof** that digital services are safe for minors should lie on the providers themselves and not on regulators, children or parents. We argue that this proof, in particular with respect to age verification and content moderation, can and should be given through independent external audits. Auditing is already present in the DSA for VLOPs and VLOSEs which need to make sure that ‘independent auditors’ assess their compliance with the DSA’s obligations.³¹ However, these audits have been criticised (Holznagel, 2025) on the grounds that some auditors refused to assess compliance with articles that were the subject of ongoing European Commission investigations, that audit criteria were not sufficiently defined; or that auditors did not conduct broad empirical testing. Such pushback by auditors may be expected in light of the economic agency problem discussed above; but for the same reason it is surprising that the DSA gives the VLOPs and VLOSEs the freedom to select their own auditors without any regulatory oversight of the process in the first place.

Age Verification

We propose a much tighter system of oversight of how high-risk service providers should carry out age verification than what is currently foreseen under EU law. Our recommendation requires **external audits and ultimately, in case the audit finds shortcomings with respect to age verification, with the involvement of the regulator, the function should be delegated to an independent third party. A further option could be that an age-verification solution is deployed at the operating system or device layer**, as already discussed in Section 5, and further below.

Introducing age verification to prevent minors from accessing harmful content online is not new and is now firmly recognised as a way to protect minors under the DSA (and under the AVMSD for VSPs). The European Commission has preliminarily found that some VLOPs have not put in place valid age checks, in breach of the DSA³². The European Commission’s guidelines on Article 28 of the DSA are also very clear that age verification should be used in four cases:

- for services that pose a high risk to minors which cannot be mitigated in another way, such as access to gambling or pornography;
- when the terms and conditions of use require the user to be at least 18;

³¹ Art. 37 DSA and Delegated Regulation 2024/436.

³² https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920,
https://ec.europa.eu/commission/presscorner/detail/en/ip_26_722.

- any circumstance where the online platform has identified risks to the privacy, safety or security of minors which cannot be mitigated by less intrusive measures;
- where EU or national law prescribes a minimum age to access a service.

Member States are expected to make available an EU-wide age verification solution by the end of 2026, according to a European Commission recommendation that was adopted in April 2026³³. Online platforms are free to choose which age verification to deploy but are encouraged to adopt double-blind age verification methods.³⁴

The current legislative framework therefore puts the responsibility of age verification on the online platform, but specifies that a tokenised approach should be adopted, which involves independent third parties that need to issue anonymised tokens. This respects the data minimisation principle, purpose limitation and user trust principles, the European Commission argued. The service providers are not supposed to carry out the age verification themselves, but they are responsible for organising it, in compliance with these principles. It is important to note that OS providers are not in scope of the DSA.

As we argued in Section 5, OS providers are oriented towards the broader ecosystem and face less direct financial pressure to compromise on neutral enforcement; even so, as we argued above, they still retain underlying commercial motives that preclude them from being fully “neutral” actors. However, the fact that the **OS provider** does not cater to any specific service provider and is instead interested in maintaining a reputation for a safe ecosystem of services makes its economic incentives **better aligned with that of child safety**. This principal insight was already recognised in the foundational work by DeAngelo (1981) in the context of the financial industry, who argues that larger (auditing) firms have more to lose from compromising their reputation for a single client, which provides an economic incentive for independence even absent regulation. However, a possible counterargument to placing age verification at the OS layer is that the existing large OS providers are already recognised as gatekeepers of the digital ecosystem under the Digital Markets Act, and their position could become further entrenched if age verification has to go through them.

We also acknowledge that **placing age verification at the OS layer requires explicit arrangements and possibly legal clarification on issues such as accountability and cost distribution**. In principle, the financial and legal costs of pursuing a risky business model should be internalised by the party that benefits from it, and should not be levied onto another party. However, OS providers should also have business incentives in their own right to offer a safe digital ecosystem for children, and bear responsibility for the services that are accessible through their infrastructure, at least to the degree to which they can exercise control over it. In most cases, there is already an economic and technical co-dependence between the OS provider and the end-service provider. After all, an OS has no economic value without services running on it, and a service requires an OS to run. In some cases, especially for OS with a high degree of openness, this relationship is informal, guided through technical standards and interfaces, rather than formal commercial agreements. However, in many cases there is also a formal contractual or economic relationship, e.g., through revenue-sharing agreements in app

³³ Commission Recommendation 2026/1035 of 29.4.2026 on establishing a common framework for EU wide Age Verification technologies.

³⁴ These methods ensure (i) that the online platform does not receive additional means to identify the user and, instead only receives information allowing it to confirm whether they meet the required age threshold and that (ii) the third party age verification provider does not obtain knowledge of the services for which the proof of age is used.

stores or developer programs, SDK license terms and other entitlements and certificates. In the latter case, agreements could be negotiated through these existing business relationships. In the former case, and only for the subset of the high-risk services – those that fail the audit – that we suggest would be required to engage a neutral third party for age verification, formal arrangements would have to be newly established.

In theory, **age verification run by a not-for-profit or governmental institution** appears to be a last option for separating financial incentives from enforcement, thereby safeguarding the integrity of protection measures. At the same time, shifting enforcement to non-commercial actors is no panacea. Government-issued applications and digital identity tools have frequently proven cumbersome, poorly maintained, and slow to incorporate technical innovation. Public-sector digital services often lag behind their commercial counterparts in usability, responsiveness to user needs, and integration with existing digital ecosystems—shortcomings that can undermine adoption and, ultimately, the effectiveness of the very protections they are meant to deliver. Many users may also not trust the government in handling their data and potentially knowing which digital services they use and how often. This suggests that neutrality achieved by removing commercial incentives altogether may come at the cost of functionality and user experience, posing its own set of trade-offs that policymakers must weigh against the benefits of reduced financial conflicts of interest.

Content Moderation

For content moderation, we do not think that entrusting an OS provider or a government-run provider is a feasible option. Assigning this to specialised, yet neutral third-party content moderation firms with clear, transparent, and audited content moderation rules seems the only logical option.

Current legal framework

The **DSA** already contains rules on content moderation³⁵ which the guidelines on Article 28 further detail to provide minors with enhanced protections. For online platforms, the guidelines specify that they also need, in particular, to:

- Clearly and transparently define what they consider as content or behaviour that is harmful for minors' privacy, safety and security, in cooperation with minors, civil society and independent experts, including academia.
- Establish moderation policies and procedures that set out how content and behaviour that is harmful for the privacy, safety and security of minors is detected and how it will be moderated aiming at limiting minors' exposure to harmful content. Online platforms also need to ensure that these policies and/or procedures are enforced in practice.
- Assess and review policies and procedures to ensure that they remain effective as technologies and online behaviours change.
- Ensure human review is available in addition to automated content review and any other relevant tools for reported accounts or content that the provider suspects may pose a risk of

³⁵ Arts 14, 15 for intermediary service; Arts 16 and 17 for hosting services; and Art 22 for online platforms only.

harm to a minor.

- Ensure that content moderation teams are well-trained and resourced and that moderation mechanisms are active and functioning at all times to deliver effective moderation, including at least one employee who is on call to respond to urgent requests.

The **European Board for Digital Services (EBDS)** has highlighted the most recurrent systemic risks and risk mitigation measures that minors are still exposed to and that the content moderation practices of VLOSES present risks (European Commission & European Board for Digital Services, 2026). In particular, they may be overly complex for children to use and, if content is not moderated in a timely manner, it could affect children disproportionately contributing to risks in relation to mental well-being. It warns that if content providers fail to accurately determine a user's age during moderation and appeals, minors may gain access to experiences or content that are not age-appropriate or may not receive protections specifically designed for younger users.

Recommendations

In light of these discussions and experiences with the DSA, we propose that content moderation for high-risk services according to our framework should be taken over by a neutral third-party in case the external audit finds shortcomings. The question remains how and by whom the content moderation firm is chosen. Here again, lessons can be learned from the rules applying to auditors in the financial industry. One may also think of levying a 'digital tax' from the service providers in question from which independent content moderation firms can be contracted by the regulator, thereby further separating financial flows from the regulated firm to the auditing firms.

Recommendation 6 (User-generated content)

For high-risk services, upload of user-generated content by children should be restricted. Restrictions can be lifted gradually (e.g., with respect to reach and vividness of content) as the child matures.

We argue that a service's systemic reliance on user-generated content (UGC) is the primary driver of conduct risk. Especially social networking services that operate as an "empty vessels" and depend almost entirely on frictionless user participation to generate demand through user-uploaded content, may have strong economic incentives that invite as much user participation and UGC as possible, which is structurally in conflict with the mitigation of the therefrom arising conduct risk. To mitigate this misalignment, the **upload of UGC by children should be restricted. In line with a developmental approach, these restrictions can be lifted gradually as the child matures**, specifically with respect to reach (who can see the uploaded content and whether the content is recommended to other users) and vividness of the content (e.g., from symbols, texts, pictures, songs to videos and livestreams).

To date, the DSA's Article 28 Guidelines do not propose to limit the upload capability of minors, except for livestreams. They only go as far as to specify that for minors' accounts, settings should ensure that by default only interaction such as likes, tags and comments by accounts that have been previously accepted should be allowed.

Specifically, we propose that **very young children should not be allowed to upload content** of their own, and the service should allow only the consumption, with complete restrictions on uploads and interactions.

As children mature, they could start to interact, using a restricted toolkit to express themselves, e.g., only being able to engage with others via texts or symbols and not via pictures and videos. Another implementation option would be to restrict the content of comments. For example, only being able to use predefined phrases without the possibility for free text or only being able to use predefined symbols and emotes also mitigates the contact risk but still gives children the possibility to have meaningful interactions in situations where interaction is vital for the core value proposition e.g., in online games.

Older adolescents would then be able to post content but expanding on previously published guidelines by the European Commission, highly vivid formats and the ability to host livestreams must be universally disabled for all minor accounts (European Commission, 2025a).

Recommendation 7 (inter-user interaction)

For high-risk services, inter-user interaction between children and peers as well as any other users should be restricted. Restrictions can be lifted gradually (e.g., with respect to reach and vividness of the interaction) as the child matures.

The features of online services that facilitate open inter-user interaction inherently expose minors to the contact risk. Because expanding the possibility and ease of contact drives network effects and engagement, service providers whose revenue generation depends on such features lack sufficient economic incentives to limit direct interaction or reduce the public reach of (young) users. Consequently, **inter-user interaction between children and others should be restricted, with limits in terms of reach and vividness of the interaction being lifted as the child matures**. Interactions should be strictly limited to previously accepted contacts, for very young users requiring parental consent, and with user profiles set to private to prevent unsolicited reach from strangers (also following the preliminary proposition by the Special Panel by Fegert & Melchior, 2026). Restrictions on reach and interaction (who can be contacted and whether profiles can be set to public) can be gradually lifted to balance online safety with the child's right to digital participation and freedom of expression.

Current legal framework

The **DSA's article 28 Guidelines** (European Commission, 2025a) only propose to limit direct messaging features to accounts that are known to minors (through default settings). The guidelines already list as a bad practice a social media platform where minors can be contacted by other users who have not been accepted as contacts by a minor. This exposes them to messages and comments by potentially malicious actors that could start engaging with them, building on emotions and gaining trust and could lead to grooming and potentially to child sexual abuse.

Likewise, although disabling direct messaging for minors is not foreseen by Article 35 of the DSA, it does encourage design choices that effectively mitigate systemic risks to children. In practice, several

VLOPs have adopted restrictions on direct messaging—ranging from limiting who can contact minors to disabling messaging altogether for younger users—as risk mitigation measures against grooming and other harmful interactions.

In March 2026, the European Commission opened formal proceedings against a social media platform for potential breach of the DSA by exposing minors to grooming attempts and recruitment for criminal purposes (European Commission (2026a)). The European Commission suspects that the platform did not adequately protect minors from being contacted by users with harmful intent.

The EBDS's second report highlights that the design and platform features of VLOPs that allow for direct messaging or encrypted messaging that facilitate private interactions can lead to sexual offenders contacting minors and facilitate grooming or solicit and distribute child sexual abuse. It also notes that private messaging functions can be used to redirect users off the platform, leading them into potentially dangerous ground. The report also notes that civil society organisations highlight that these tools are also an important safeguard to ensure the effectiveness of freedom of expression.

Recommendation 8 (exposure to experimental technology)

For high-risk services, the exposure of children to experimental technology (such as generative AI) should be limited. Restrictions can be gradually lifted, as the child matures.

As established in our framework, a service's systemic reliance on experimental technology such as generative AI introduces risks rooted in technical unpredictability. However, it also depends on to which context the technology is used and how it drives revenue generation. For example, it matters whether the service is ad-financed and has incentives to keep users online as long as possible, which would then provide incentives to create AI dependency and addiction. Likewise, it matters what type of content is created by the technology, e.g., whether the AI can create videos and images that are age inappropriate. We therefore posit that **children should not be prohibited from using experimental technology per se, but that their exposure should be limited, especially when the overall risk profile of the service is high; and that the technology needs to pass higher safety standards when children can interact with it.** In line with a developmental approach, these restrictions can be gradually lifted as the child matures, provided that safety guidelines are met, and explicit disclaimers denote the risks. Features that are explicitly designed to foster emotional dependence should never be allowed for children.

This is a novel idea from a regulatory perspective. AI is certainly the most recent example of how an experimental technology has been rapidly deployed and has affected our everyday lives. The current regulatory tools have been put to the test and although the European Commission was quick to communicate on the potential dangers, minors have been exposed to the technology although they are likely to be particularly exposed to danger. The classification of generative AI and AI assistants has recently been addressed under the DSA. The European Commission designated ChatGPT as a very large online search engine on 31 August 2026. For the purpose of this report, this means that Article 28 does not apply to ChatGPT, although the risk management obligations do apply. The **EBDS's second report on systemic risks** (European Commission & European Board for Digital Services, 2026) has recognised that systemic risks can be mitigated or aggravated by several factors. It explicitly

acknowledges “that business models aimed at maximising user engagement and time spent on a service may lead providers of VLOPs and VLOSEs to make design choices that may aggravate systemic risks, including in relation to the protection of minors”. Generative AI is listed as one of these risk factors that can be used in ways that can be harmful to minors. The spread of AI generated content on VLOPs and VLOSEs (e.g., AI generated sexual deepfakes of women and minors have been widely disseminated on some VLOPs and VLOSEs) and the use of AI assistants (with potential impacts on the mental well-being of minors and on the dissemination of child sexual abuse material, CSAM) have increased risks for minors. It also mentions that civil society organisations have raised that Gen AI is a risk factor in relation to CSAM risks.

The **European Commission’s Guidelines on Article 28** have highlighted that AI assistants and companions that “have been integrated” into online platforms could present risks to the privacy, safety and security of minors. The European Commission opened a formal investigation to assess if X may have breached its risk management obligation when it deployed its AI chatbot Grok in the EU. As reported (Center for Countering Digital Hate, 2026), Grok generated 3m sexualised images, including 23000 that appear to depict children, over an 11-day period. The case was opened on 26 January 2026; i.e., after these images were generated.

This shows that the European Commission appears to be grappling with how to apply the DSA to generative AI and that children have been exposed to harm. The enforcement of the AI Act is yet to be tested.

7.4. Summary

Finally, we critically assess our recommendations against existing EU law and identify gaps in the protection of children online that should be addressed by future regulation, summarised in Table 1.

Table 1: Summary of recommendations and mapping to existing EU law

Proposed Recommendation	Parts already covered by EU regulation	Parts not covered by EU regulation
Rec. 1: Regulation should scale with the risk that the service’s business model creates for children	Current rules only cater for this approach marginally and indirectly (DSA in particular).	No holistic and express approach covering all services.
For all services		
Rec. 2: Strict advertising limitations	Quantitative and qualitative limits on advertising for linear, non-linear services and for VSP’s own advertising (AVMSD). No targeted advertising for minors (DSA).	No quantitative and qualitative limits on advertising for other services than those covered under the AVMSD. No prohibition of targeted advertising for services other than online platforms (as defined in the DSA).
Rec. 3: No opaque monetisation strategy	Rules on transparency of advertising exist under EU legislation (DSA, AVMSD, Ecom Directive, PAR). Some rules on digital contracting (duration, termination, dark patterns) exist under consumer protection legislation and the DSA.	No general rule on transparency of monetisation strategy. Virtual currencies, loot boxes and probability-based monetisation not clearly covered. Prohibition of auto-renewals based on dark patterns for all services.
Rec. 4: Restrictions on collection of personal data	When data processing is based on consent, consent needs to be given by parents/guardians when children are below 16 (or 13 depending on the Member State, GDPR).	No general prohibition (covering all services) to: further process personal data (collected initially to protect minors)

	General requirement for online platforms to ensure a high level of safety, privacy and security of minors (DSA). No further processing (for commercial purposes) of personal data collected to protect them (AVMSD and DSA). No targeted advertising for minors (DSA).	• prompt minors or legal guardians to consent to more extensive data collection • address targeted advertising to minors
For high-risks services		
Rec. 5: External audits on age assurance and content moderation and functions to be delegated to neutral third party in case of shortcomings	Auditing of VLOPS and VLOSEs's obligations is foreseen under the DSA	Delegation of function is not currently covered or envisioned under EU regulation
Rec. 6: Restrictions on upload functions by children	Restrictions on uploads of livestreams (Art.28 DSA guidelines). Default settings to allow for interactions with previously accepted accounts (Art.28 DSA guidelines).	No general prohibition to upload content and to interact for very young children on all services
Rec. 7: Restrictions on inter-user interaction	Default settings to allow for interactions with previously accepted accounts (Art.28 DSA guidelines). Could be a mitigating measure for VLOPs and VLOSEs (DSA)	No general prohibition of inter-user interaction on all services
Rec. 8: Limits on exposure to experimental technology	-	New idea not currently covered or envisioned under EU regulation

Our framework aligns with the core philosophy of the Digital Services Act (DSA) in that services that bear high risk and maintain a large user base require stricter regulation. However, the DSA does not account for underlying business-model incentives and applies only to a subset of the services that exhibit a high-risk profile in our framework – leaving out significant online environments, such as certain monetisation models applied in video games.

As the summary table shows, current EU legislation already addresses some of the recommendations put forward in the report but in a piecemeal and indirect manner and in most cases in relation to certain services only. If followed, **most of the recommendations could be translated into new EU-level legislation on the protection of minors online, preferably into a Regulation.**

The option of amending the DSA is not recommended, since the scope of the DSA is strictly limited to certain services.

If such a new EU legislation on the protection of minors online is adopted, we recommend – in a spirit of simplification of the legal framework, that the sector-specific rules are removed (in particular Article 28 of the DSA).

The upcoming DFA would probably be an adequate legal instrument to address measures proposed in Recommendation 3 (opaque monetisation).

8. Conclusions

In this paper we propose a novel framework that bridges the gap between digital service design and regulatory intervention by mapping seven core business model dimensions directly to the OECD's typology of risks online. By focusing on fundamental economic drivers rather than specific interface design features that arise as a consequence thereof, our framework offers a future-proof approach to evaluating a service's risk profile that operates independently of existing, often rigid, legal categorisations.

We arrive at several key findings and actionable implications for the governance of online services. First, regarding targeted oversight for high-risk services, regulation should primarily target services characterised by both a high user base and a high risk profile (Recommendation 1). For these high-risk services, regulatory intervention must focus on reducing underlying business incentives to generate risk, effectively realigning service incentives to lower their risk profiles across the seven business model dimensions (Recommendations 5-8). While high-risk services require targeted intervention, certain financial dependencies on usage duration and opaque monetisation strategies must be universally curtailed. Systemic financial incentives to prolong usage duration, deploy opaque monetisation mechanics, or exploit children's personal data must be restricted across all services, regardless of their overall risk profile (Recommendation 2-4).

In alignment with the recommendations of the EU Special Panel (Fegert & Melchior, 2026), we also advocate for a developmental approach to digital safety. Rather than applying blunt bans, policy frameworks should allow restrictions on certain services to be gradually lifted as children mature and gain resilience and digital literacy. Crucially, our framework offers a nuanced alternative to blanket service bans, such as the recently announced social media bans for minors. Under our model, social networking services are unmistakably classified as high-risk due to their reliance on ad-supported monetisation, opaque pricing, high reliance on user-generated (and potentially harmful) content, extensive data collection, and unmediated inter-user interaction. However, instead of excluding young users entirely, applying our recommendations to social media services could reshape how these services operate to make them safer for children. This includes enforcing strict limits on (targeted) advertising, user-generated content uploads, inter-user interactions, and data collection. In some high-risk cases, to realign incentives and counteract misconduct, these services may also be mandated to externalise age verification to neutral third parties. In contrast to a ban, these restrictions allow service providers to design a safer service for children overall, effectively reducing their risk-profile in exchange for less heavy-handed regulation.

In closing, we emphasise again that our novel framework and the recommendations in this report should be considered as foundational new thinking on the topic of child protection online, outlining a different path that EU regulation can (and in our view should) pursue in order to move beyond fragmented, feature-based interventions and towards addressing the underlying economic drivers that make exposing children to digital risks profitable in the first place. By realigning financial incentives with user safety like we propose in this report, regulation can foster a digital ecosystem that protects children without foreclosing their participation completely. However, given we are breaking new ground with these ideas, our report is not the definitive conclusion, but hopefully rather a fruitful starting point for such legislative change.

9. References

- 5Rights Foundation. (2021). Pathways: How digital design puts children at risk. <https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf>
- Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2020). The Welfare Effects of Social Media. *American Economic Review*, 110(3), 629–676.
- Anderson, S. P., & Coate, S. (2005). Market Provision of Broadcasting: A Welfare Analysis. *Review of Economic Studies*, 72(4), 947–972.
- Anderson, S. P., & Jullien, B. (2015). The Advertising-Financed Business Model in Two-Sided Media Markets. In *Handbook of Media Economics*, Vol. 1A, 41–90. Elsevier.
- Apple (2026). *Apple Developer Program: Membership details*. Apple Developer. <https://developer.apple.com/help/app-store-connect/making-payments-to-apple/overview-of-making-payments-to-apple>
- Aridor, G., Che, Y.-K., & Salz, T. (2023). The effect of privacy regulation on the data industry: Empirical evidence from GDPR. *RAND Journal of Economics*, 54(4), 695–730. <https://doi.org/10.1111/1756-2171.12455>
- Aridor, G., Jiménez Durán, R., Levy, R., Song, L. (2024). The Economics of Social Media. *Journal of Economic Literature*, 62 (4): 1422–74. <http://dx.doi.org/10.2139/ssrn.4708840>
- Bajari, P., Chernozhukov, V., Hortaçsu, A., & Suzuki, J. (2019). The impact of big data on firm performance: An empirical investigation. *AEA Papers and Proceedings*, 109, 33–37. <https://doi.org/10.1257/pandp.20191000>
- Beltrán, M. (2025). Defining, Classifying and Identifying Addictive Patterns in Digital Products. *IEEE Transactions on Technology and Society*, 6(3): 314–323. <https://doi.org/10.1109/TTS.2025.3564840>
- Bergemann, D., Bonatti, A., & Gan, T. (2022). The economics of social data. *RAND Journal of Economics*, 53(2), 263–296. <https://doi.org/10.1111/1756-2171.12407>
- Bhargava, V. R., & Velasquez, M. (2021). Ethics of the attention economy: The problem of social media addiction. *Business Ethics Quarterly*, 31(3), 321–359. <https://doi.org/10.1017/beq.2020.32>
- Boyer, R. (2022). Platform capitalism: A socio-economic analysis. *Socio-Economic Review*, 20(4), 1857–1879. <https://doi.org/10.1093/ser/mwaa055>
- Brooks, G. A., & Clark, L. (2019). Associations between loot box use, problematic gaming and gambling, and gambling-related cognitions. *Addictive Behaviours*, 96, 26–34. <https://doi.org/10.1016/j.addbeh.2019.04.009>
- Buiten, M., & Busch, C. (2025). *Protection of minors: Age-appropriate design under the Digital Services Act*. Centre Regulation in Europe (CERRE). <https://cerre.eu/publications/protection-of-minors-age-appropriate-design/>
- Burszty, L., Duckworth, A., Jiménez-Durán, R., Leonard, A., Milojevic, F., Roth, C. & Sunstein, C. R. (2026). Why Bans Fail: Tipping Points and Australia’s Social Media Ban. *BFI Working Paper*, No. 2026-57. Becker Friedman Institute for Economics. https://bfi.uchicago.edu/wp-content/uploads/2026/04/BFI_WP_2026-57.pdf
- Busch, C., Fletcher, A., & Ledger, M. (2026). *Towards an EU Consumer Law fit for the digital age*. Centre on Regulation in Europe (CERRE). <https://cerre.eu/wp-content/uploads/2025/03/CERRE-DSA-Forum-Age-Appropriate-Design.pdf>

- Busch, C., & Fletcher, A. (2024). *Harmful online choice architecture*. Centre Regulation in Europe (CERRE). <https://cerre.eu/publications/harmful-online-choice-architecture/>
- Calvert, S. L. (2008). Children as consumers: Advertising and marketing. *The Future of Children*, 18(1), 205–234. <https://doi.org/10.1353/foc.0.0001>
- Cameran, M., Prencipe, A., & Trombetta, M. (2016). Mandatory audit firm rotation and audit quality. *European Accounting Review*, 25(1), 35–58. <https://doi.org/10.1080/09638180.2014.921446>
- Center for Countering Digital Hate (2026). Grok floods X with sexualised images of women and children. <https://counterhate.com/research/grok-floods-x-with-sexualised-images/>
- Conseil constitutionnel. (2026, August 14). Décision n° 2026-911 DC du 14 août 2026, Loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux. <https://www.conseil-constitutionnel.fr/decision/2026/2026911DC.htm>
- Cordes, S., Dertwinkel-Kalt, M., & Werner, T. (2024). What drives demand for loot boxes? An experimental study. *Journal of Economic Behaviour & Organisation*, 228. <https://doi.org/10.1016/j.jebo.2024.106755>
- DeAngelo, L. E. (1981). Auditor size and audit quality. *Journal of Accounting and Economics*, 3(3), 183–199. [https://doi.org/10.1016/0165-4101\(81\)90002-1](https://doi.org/10.1016/0165-4101(81)90002-1)
- De Freitas, J., Castelo, N., Uğuralp, A. K. & Oğuz-Uğuralp, Z. (2025) Lessons from an app update at Replika AI: identity discontinuity in human-AI relationships. *Working paper 25-018*, Harvard Business School. https://www.hbs.edu/ris/Publication%20Files/25-018_bed5c516-fa31-4216-b53d-50fedda064b1.pdf
- De Freitas, J., & Cohen, I. G. (2025). Unregulated emotional risks of AI wellness apps. *Nature Machine Intelligence*, 7, 813-815. <https://doi.org/10.1038/s42256-025-01051-5>
- Demski, J. S. (2003). Corporate Conflicts of Interest. *Journal of Economic Perspectives*. 17(2), 51-72. <https://doi.org/10.1257/089533003765888421>
- Dertwinkel-Kalt, M., Normann, H.-T., Werner, T., & Tiede, J.-N. (2025). Deceptively Framed Lotteries in Consumer Markets. Available at SSRN: <https://ssrn.com/abstract=5699082>
- Engels, B., & Potthoff, J. (2025). Social Media, Markets and Minors: A Behavioural Ethics Perspective. German Economic Institute. *IW-Policy Paper*, 12, <https://www.iwkoeln.de/en/studies/barbara-engels-jennifer-potthoff-a-behavioural-ethics-perspective.html>
- Esposito, F., & Cathoud Ferreira, T. M. (2024). Addictive design as an unfair commercial practice: The case of hyper-engaging dark patterns. *European Journal of Risk Regulation*, 15(4), 999–1016. <https://doi.org/10.1017/err.2024.8>
- European Commission (2024a). Commission opens formal proceedings against TikTok under the Digital Services Act. Press Release. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926
- European Commission (2024b). Review of EU consumer law. https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en
- European Commission (2025a). Commission publishes guidelines on the protection of minors. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>
- European Commission. (2025b). A simpler and faster Europe: Communication on implementation and simplification (COM(2025) 47 final)

- European Commission (2026a). Digital Services Act: Commission opens formal proceedings against Snapchat over risks to minors. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_723
- European Commission (2026b). European Commission. (2026, August 31). [Commission designates ChatGPT, Reddit, Roblox under Digital Services Act.](#)
- European Commission & European Board for Digital Services. (2026). *Second report on systemic risks on very large online platforms and search engines under the Digital Services Act*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services>
- Fegert, J. M., & Melchior, M. (2026). Child safety online: Protecting and empowering minors in a digital world (Report by the Co-Chairs of the Special Panel on Child Safety Online). European Commission. https://commission.europa.eu/document/download/d833504d-5ec3-4fac-945f-38e7d0bd5326_en?filename=Special-panel-report.pdf
- Feijoo, B., & Sádaba, C. (2022). When ads become invisible: Minors' advertising literacy while using mobile phones. *Media and Communication*, 10(1), 339–349. <https://doi.org/10.17645/mac.v10i1.4720>
- Flayelle, M., Brevers, D., King, D. L., Maurage, P., Perales, J. C., & Billieux, J. (2023). A taxonomy of technology design features that promote potentially addictive online behaviours. *Nature Reviews Psychology*, 2, 136–150. <https://doi.org/10.1038/s44159-023-00153-4>
- de Fortuny, E. J., Martens, D., & Provost, F. (2013). Predictive modeling with big data: Is bigger really better? *Big Data*, 1(4), 215–226. <https://doi.org/10.1089/big.2013.0037>
- Frankel, R. M., Johnson, M. F., & Nelson, K. K. (2002). The relation between auditors' fees for nonaudit services and earnings management. *The Accounting Review*, 77(s-1), 71–105. <https://doi.org/10.2308/accr.2002.77.s-1.71>
- Galissaire, J. (2025) Policy Brief, Mind the Gap, Age Assurance and the Limits of Enforcement under EU Law. <https://www.interface-eu.org/publications/age-assurance-gap>.
- Gath, M., & Swit, C. (2024). Digital media in early childhood: risk factors for online harm and psychosocial correlates. *Frontiers in Developmental Psychology*, 2, 1390276. <https://doi.org/10.3389/fdpys.2024.1390276>
- Garg, A., Goel, P., Rana, N. P., Mishra, A. (2026). AI Beauty Filters, and Appearance Self-Esteem: An Empirical Investigation. *Journal of Consumer Behaviour*, 25 (4), 1678-1700. <https://doi.org/10.1002/cb.70141>.
- Germano, F., Gómez, V., & Sobbrío, F. (2026). Ranking for engagement: How social media algorithms fuel misinformation and polarisation. *Journal of Public Economics*. 255. <https://doi.org/10.1016/j.jpubeco.2026.105589>
- Goldfarb, A., & Tucker, C. (2019). Digital economics. *Journal of Economic Literature*, 57(1), 3–43. <https://doi.org/10.1257/jel.20171452>
- Google (2026). *Service fees*. Play Console Help. <https://support.google.com/googleplay/android-developer/answer/112622?hl=en>
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). Association for Computing Machinery. <https://doi.org/10.1145/3173574.3174108>

- Holznagel, D. (2025). Shortcomings of the first DSA Audits — and how to do better. <https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/>
- Hu, B., Mao, Y., Kim, K. J. (2023). How social anxiety leads to problematic use of conversational AI: The roles of loneliness, rumination, and mind perception. *Computers in Human Behaviour*, 145. <https://doi.org/10.1016/j.chb.2023.107760>
- Huang, S., Lai, X., Ke, L., Li, Y., Wang, H., Zhao, X., Dai, X., Wang, Y. (2024). AI Technology panic-is AI Dependence Bad for Mental Health? A Cross-Lagged Panel Model and the Mediating Roles of Motivations for AI Use Among Adolescents. *Psychology Research and Behaviour Management*, 17. <https://doi.org/10.2147/PRBM.S440889>
- Ibáñez-Sánchez, S., Orús, C., & Flavián, C. (2022). Augmented reality filters on social media. Analyzing the drivers of playability based on uses and gratifications theory. *Psychology & Marketing*, 39, 559–578. <https://doi.org/10.1002/mar.21639>
- Ichihashi, S., & Kim, B.-C. (2022). Addictive Platforms. *Management Science*, 69(2). <https://doi.org/10.1287/mnsc.2022.4392>
- IEEE. (2021). *IEEE standard for an age appropriate digital services framework based on the 5Rights principles for children* (IEEE Std 2089-2021). IEEE Standards Association. <https://doi.org/10.1109/IEEESTD.2021.9627644>
- Internet Matters. (2026). The Online Safety Act: Are children safer online?. <https://www.internetmatters.org/wp-content/uploads/2026/04/Internet-Matters-Online-Safety-Act-Report-May-2026.pdf>
- Johnson, G. A., Shriver, S. K., & Du, S. (2020). Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science*, 39(1), 33–51. <http://dx.doi.org/10.2139/ssrn.3020503>
- Johnson, G. A., Lin, T., Zhong, L., & Cooper, J. C. (forthcoming). COPPAcalypse? The YouTube settlement's impact on kids content. Accepted at Management Science. <https://doi.org/10.1287/mnsc.2024.05295>
- King, D. L., & Delfabbro, P. H. (2018). Predatory monetisation schemes in video games (e.g., 'loot boxes') and internet gaming disorder. *Addiction*, 113(11), 1967–1969. <https://doi.org/10.1111/add.14286>
- Klein, T., Kurmangaliyeva, M., Prüfer, J., & Prüfer, P. (2022). How important are user-generated data for search result quality? Experimental evidence. *TILEC Discussion Paper*. No 2022- 016 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4229292
- Krämer, J., & Schnurr, D. (2022). Big data and digital markets contestability: Theory of harm and data access remedies. *Journal of Competition Law & Economics*, 18(2), 255-322. <https://doi.org/10.1093/joclec/nhab015>
- Krämer, J. & Shekhar, S. (2025). Regulating Digital Platform Ecosystems Through Data sharing and Data Siloing: Consequences for Innovation and Welfare. *MIS Quarterly*, 49 (1): 123–154. <https://doi.org/10.25300/MISQ/2024/18428>
- Kumar, S., Sharma, V., & Agarwal, A. (2026). Curbing Hidden Advertisements in Children's Videos: The Limits of Platform Policies. Working Paper. https://questromworld.bu.edu/platformstrategy/wp-content/uploads/sites/49/2026/06/1164_Sharma_Youtube_Hidden_Ads_Sumeet_Vasundhara_Ashish.pdf

- Laestadius, L., Bishop, A., Gonzalez, M., Illenčik, D., Campos-Castillo, C. (2024). Too human and not human enough: A grounded theory analysis of mental health harms from emotional dependence on the social chatbot Replika. *New Media & Society*, 26(10). <https://doi.org/10.1177/14614448221142007>
- Ledger, M. (2026). Transatlantic cooperation on protecting minors online (Issue Paper). Centre on Regulation in Europe (CERRE). <https://cerre.eu/publications/transatlantic-cooperation-on-protecting-minors-online/>
- Li, Y., & Xie, Y. (2020). Is a Picture Worth a Words? An Empirical Study of Image Content and Social Media Engagement. *Journal of Marketing Research*, 57(1), 1-19. <https://doi.org/10.1177/0022243719881113>
- Liu, Y., Yildirim, T. P., & Zhang, Z. J. (2022). Implications of Revenue Models and Technology for Content Moderation Strategies. *Marketing Science*. 41(4). <https://doi.org/10.1287/mksc.2022.1361>
- Livingstone, S., & Smith, P. K. (2014). Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654. <https://doi.org/10.1111/jcpp.12197>
- Livingstone, S., & Third, A. (2017). Children and young people’s rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–670. <https://doi.org/10.1177/1461444816686318>
- Manolios, S.; Chaudron, S.; Sala, A.; Gomez, E. (2026): Online Minor Protection Matrix. European Commission, Joint Research Centre [Dataset]. <https://10.2905/JRC.XHBGN5G>
- Miao, J., & Jain, S. (2024). Designing loot boxes: Implications for profits and welfare. *Marketing Science*, 43(6), 1242–1259. <https://doi.org/10.1287/mksc.2023.0007>
- Milli, S., Carroll, M., Wang, Y., Pandey, S., Zhao, S., & Dragan, A. D. (2025). Engagement, user satisfaction, and the amplification of divisive content on social media. *PNAS nexus*, 4(3). <https://doi.org/10.1093/pnasnexus/pgaf062>
- Montag, C., Lachmann, B., Herrlich, M., & Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International Journal of Environmental Research and Public Health*, 16(14). <https://doi.org/10.3390/ijerph16142612>
- Munzer, T., Parga-Belinkie, J., Milkovich, L. M., Tomopoulos, S., Ajumobi, T., Cross, C., Gerwin, R., Madigan, S., & Council on Communications and Media. (2024). Digital ecosystems, children, and adolescents: Policy statement. *Pediatrics*, 154(1). <https://doi.org/10.1542/peds.2025-075320>
- OECD. (2012). Market definition (OECD Series Roundtables on Competition Policy No. 130) <https://doi.org/10.1787/62f0f46c-en>
- OECD. (2021). Children in the digital environment: Revised typology of risks (OECD Digital Economy Papers No. 302). <https://doi.org/10.1787/9b8f222e-en>
- OECD. (2025). How’s life for children in the digital age? (OECD Publishing, Paris). <https://doi.org/10.1787/0854b900-en>
- O’Neill, B. (2023). Research for CULT Committee – The influence of social media on the development of children and young people. European Parliament, Policy Department for Structural and Cohesion Policies.

- Petrovskaya, E., & Zendle, D. (2022). Predatory monetisation? A categorisation of unfair, misleading and aggressive monetisation techniques in digital games from the player perspective. *Journal of Business Ethics*, 181, 1065–1081. <https://doi.org/10.1007/s10551-021-04970-6>
- Phang, J., Lampe, M., Ahmad, L., Agarwal, S., Fang, C. M., Liu, A. R., Danry, V., Lee, E., Chan, S. W. T., Pataranutaporn, P., & Maes, P. (2025). Investigating Affective Use and Emotional Well-Being on ChatGPT. Available on: <https://arxiv.org/abs/2504.03888v1>
- Prat, A., & Valletti, T. (2022). Attention Oligopoly. *American Economic Journal: Microeconomics*, 14(3), 530–557.
- Prelec, D., & Loewenstein, G. (1998). The Red and the Black: Mental accounting of savings and debt. *Marketing Science*, 17, 4–28. <https://doi.org/10.1287/mksc.17.1.4>
- Prüfer, J., & Schottmüller, C. (2021). Competing with big data. *The Journal of Industrial Economics*, 69(4), 967–1008. <https://doi.org/10.1111/joie.12259>
- Raghubir, P., & Srivastava, J. (2008). Monopoly money: The effect of payment coupling and form on spending behaviour. *Journal of Experimental Psychology: Applied*, 14(3), 213–225. <https://doi.org/10.1037/1076-898X.14.3.213>
- Ribeiro, M. H., Ottoni, R., West, R., Almeida, V. A. F., Meira, W. (2020). Auditing radicalisation pathways on YouTube. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 131–141. <https://doi.org/10.1145/3351095.3372879>
- Riedel, A., Mulcahy, R., Beatson, A., & Weeks, C. (2025). Advertising in Freemium Services: Lack of Control and Intrusion as the Price Consumers Pay. *Journal of Advertising*, 54(3), 322–341. <https://doi.org/10.1080/00913367.2024.2393078>
- Robayo-Pinzon, O., Rojas-Berrio, S., Camargo, J.E. and Foxall, G.R. (2025). Generative artificial intelligence (GenAI) use and dependence: an approach from behavioural economics. *Frontiers in Public Health*, 13. <https://doi.org/10.3389/fpubh.2025.1634121>
- Sas, M., & van der Hof, S. (2025). Digital games, a missed target of the Digital Services Act? *Auteurs & Media*, 2025(2), 132–146.
- Schaefer, M., & Sapi, G. (2023). Complementarities in learning from data: Insights from general search. *Information Economics and Policy*, 65, <https://doi.org/10.1016/j.infoecopol.2023.101063>
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. *EU Kids Online*. <https://doi.org/10.21953/lse.47fdeqj01ofo>
- Steuer, J. (1992). Defining Virtual Reality: Dimensions Determining Telepresence. *Journal of Communication*, 42: 73–93. <https://doi.org/10.1111/j.1460-2466.1992.tb00812.x>
- Stoilova, M., Bulger, M., & Livingstone, S. (2024). Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use. *Journal of Children and Media*, 18(1), 29–49. <https://doi.org/10.1080/17482798.2023.2265512>
- UNESCO (2026). Growing up in a connected world: A family guide for the digital age (UNESCO Publishing). <https://unesdoc.unesco.org/ark:/48223/pf0000398455.locale=en>
- UNICEF (2025). Childhood in a Digital World: Screen time, digital skills and mental health (UNICEF Innocenti). <https://www.unicef.org/innocenti/media/11296/file/UNICEF-Innocenti-Childhood-in-a-digital-world-report-2025.pdf>

- United Nations General Assembly. (1989). Convention on the Rights of the Child (Resolution 44/25). <https://www.ohchr.org/sites/default/files/crc.pdf>
- U.S. Securities and Exchange Commission. (2003). Strengthening the Commission's requirements regarding auditor independence. <https://www.sec.gov/rules-regulations/2003/01/strengthening-commissions-requirements-regarding-auditor-independence>
- Valkenburg, P. M., van Driel, I. I., & Beyens, I. (2022). The associations of active and passive social media use with well-being: A critical scoping review. *New Media & Society*, 24(2), 530–549. <https://doi.org/10.1177/14614448211065425>
- Verduyn, P., Gugushvili, N., & Kross, E. (2022). Do Social Networking Sites Influence Well-Being? The Extended Active-Passive Model. *Current Directions in Psychological Science*, 31(1), 62–68. <https://doi.org/10.1177/09637214211053637>
- Wardle, H., & Zendle, D. (2021). Loot boxes, gambling, and problem gambling among young people: Results from a cross-sectional online survey. *Cyberpsychology, Behaviour, and Social Networking*, 24(4), 267–274. <https://doi.org/10.1089/cyber.2020.0299>
- Xie, T., Pentina, I., Hancock, T. (2023). Friend, mentor, lover: does chatbot engagement lead to psychological dependence?. *Journal of Service Management*, 34(4). <https://doi.org/10.1108/JOSM-02-2022-0072>
- Yoganarasimhan, H. (2020). Search personalisation using machine learning. *Management Science*, 66(3), 1045–1070. <https://doi.org/10.1287/mnsc.2018.3255>
- Yu, S.-C., Chen, H.-R., Yang, Y.-W. (2024). Development and validation the Problematic ChatGPT Use Scale: a preliminary report. *Current Psychology*, 43, 26080 – 26092. <https://doi.org/10.1007/s12144-024-06259-z>
- Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020). The prevalence of loot boxes in mobile and desktop games. *Addiction*, 115(9), 1768–1772. <https://doi.org/10.1111/add.14973>
- Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

About CERRE

Providing high-quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network, digital industry, and service sectors. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g., energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.

About the Authors



Jan Krämer is a CERRE Academic Co-Director and Professor for Information Systems at the University of Passau, Germany, where he holds the Chair for Internet & Telecommunications Business. He has a diploma degree in Business Engineering and Management, and a Ph.D. in Economics, both from the Karlsruhe Institute of Technology. He has published numerous articles in the leading journals in the areas of Information Systems, Economics and Marketing. His current research interests include the regulation of platforms and internet markets, as well as digital ecosystems and data-driven business models.



Michèle Ledger is a CERRE Research Fellow and researcher at the Research Centre in Information, Law and Society (CRIDS) of the University of Namur where she also lectures on the regulatory aspects of online platforms at the postmaster degree course. She has been working for more than twenty years at Cullen International and leads the company's Media regulatory intelligence service.



Sonja Herrmann is a Ph.D. student in Information Systems at the Chair for Internet & Telecommunications Business and in the DFG-funded Research Training Group Digital Platform Ecosystems, both at the University of Passau, Germany. Prior to that she completed her studies with a master's degree in business administration also at the University of Passau. In her research she focuses on the intersection between digital platform monetisation, behavioural design and consumer protection, especially in the context of video game design mechanics.

cerre



Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

 Centre on Regulation in Europe (CERRE)
 CERRE Think Tank
 CERRE Think Tank