Are EU Kidding Me? Notes from a Poorly Drafted Social Media Ban

Michael Veale*

Faculty of Laws, UCL and IViR, University of Amsterdam

Cite as: 11 Geo. L. Tech. Rev. _ (2026)
(2026) 11 Georgetown Law Technology Review _
doi.org/10.31235/osf.io/fwjpq_v3
files.michae.lv/papers/veale_areEUkiddingme.pdf

November 7, 2026
First version posted 1 October 2026

ABSTRACT

In September 2026, the European Commission published a proposed EU KIDS Act, responding to the demand for restrictions and further design obligations applying to digital services accessible to children, including social media. This Article argues that regardless of what one believes about the merits of this policy direction, the EU KIDS Act is not the legislative text we need. The scope and drafting are little short of chaotic and full of holes, enormous ambiguities, and unintended consequences. Recitals contradict articles. The use of borrowed scope definitions from other pieces of legislation not designed for this purpose brings services into scope that should not be subject to the relevant provisions, like book-recommendation websites, music services, or exercise trackers. The infrastructural requirement for age assurance and parental responsibility attestation simply omits enormous issues of complex families and childhoods. Complex design obligations are written in ways that can be plausibly interpreted as implicitly prohibiting entire swathes of products, such as voice assistants. This Article outlines these issues, and many more. The Commission should withdraw this proposal and reissue a workable and realistic text.

---

*: Professor of Technology Law and Policy, Faculty of Laws, University College London; Fellow, Institute for Information Law, University of Amsterdam; Global Professor of Law, New York University School of Law (2026–7). This Article has not been presented at lots of places and sent around to lots of friendly and impressive people as it has been written quite rapidly to respond to the draft and to try and impact upon the legislative process. Special thanks, however, go to Tommaso Fia for flagging the draft just before a long-haul plane journey so I could analyze it in peaceful shock, and for his titular assistance. Thanks also go to Catalina Goanta for useful input on later versions. Further thanks also go to the editorial team at GLTR for their exceptional work, which strengthened this Article.

CONTENTS

I. Introduction **3**
- A. Access . . . 5
- B. Design . . . 5
- C. Infrastructure . . . 6
- D. Scope . . . 6
  - 1. Territorial Scope . . . 6
  - 2. “Accessible to Minors” . . . 7
- E. Compliance and Enforcement . . . 8

II. Specific Services **9**
- A. Online Social Networking and Video Sharing Platform Services . . . 9
  - 1. These Aren’t the Platforms You’re Looking For . . . 10
  - 2. Escaping the Scope . . . 11
- B. Online Games . . . 11
  - 1. Online Games Include All Offline Games? . . . 12
  - 2. Social Networks in Trenchcoats . . . 13
  - 3. Loot Boxes Banned in All Services Except Games . . . 14
- C. AI Systems . . . 14
  - 1. Exempting Educational Chatbots . . . 14
  - 2. Inherently Dependable Companions . . . 15
- D. Software Application Stores . . . 16
  - 1. Shared Devices . . . 16
  - 2. What’s in Store? Who Cares? . . . 17
  - 3. An Accidental Book Ban? . . . 17

III. When a Setting Becomes a Ban **18**

IV. Awkward Realities of Age Assessment **21**
- A. Age Assurance . . . 21
- B. Age Assurance… Without Data? . . . 22
- C. When It Goes Wrong . . . 24
- D. Or Just Times Out . . . 24

V. Tooled-Up Guardians **25**
- A. Who Are the Guardians? Problems of Parental Attestation . . . 25
  - 1. Defining the Guardians . . . 25
  - 2. Look Mom, No Data . . . 26
  - 3. The Politics of Pan-European Parenthood . . . 27
  - 4. Expect Self-Declaration . . . 27
- B. The Long Tail of Kids and Families . . . 28
- C. One API per Child . . . 29
- D. Stalkerware Paradise . . . 30

VI. Designing Good Content In and Bad Content Out **31**
A. What If the Kids Want a Filter Bubble? 32
B. It's Not General Monitoring, It's Detection by Design 32

VII. Conclusion: Revise and Resubmit **33**
A. Shift the Scope 34
B. Embrace the Chaos 34
C. Security Is Not the Aim 35

I. INTRODUCTION

Political momentum has been growing for legislators to respond to the very real concerns that corporate technology providers have a level of access to and influence over children that is detrimental both to them and to society as a whole. There is now a long and meandering heritage of different jurisdictions attempting to regulate children's experiences online.

Some of these attempts concern design obligations on social media platforms. In the United States, the high-profile consent judgment and settlement agreement in August 2026 between Meta and fifty-one state and territorial attorneys general is the latest step in regulatory efforts.[1] This settlement is important less for its payout than for its significant conduct obligations. Many of these enshrine or resurrect parts of California's Protecting Our Kids from Social Media Addiction Act, including those that have been subject to ongoing First Amendment challenges.[2] The obligations in this settlement include provisions that require Meta, for users under 18 on its social media platforms, to (a) impose audited age assurance and attempt to detect children under 13; (b) hide or mute certain addictive or distracting features; and (c) impose a daily usage cap and overnight lockout.[3] Similar design obligations have also been created in jurisdictions such as the United Kingdom.[4]

Another strand of this history is the growing momentum for a prohibition on certain social media services for children. This arguably began in Australia with a law that was rapidly passed in 2024.[5] In Europe, several countries have recently proposed social media bans of varying flavors. However,

1: Settlement Agreement § II.B.3(a)(i), California v. Meta Platforms, Inc., No. 4:23-cv-05448-YGR (N.D. Cal. Aug. 26, 2026) [hereinafter Settlement Agreement].

2: Protecting Our Kids from Social Media Addiction Act, Cal. Health & Safety Code §§ 27000-27007 (West 2026); *see, e.g.*, NetChoice, LLC v. Bonta, 152 F.4th 1002, 1016 (9th Cir. 2025) (relating to rules regarding "like" counts on Facebook).

3: Settlement Agreement, *supra* note 1, § II.

4: Online Safety Act 2023, c. 50, §§ 11–13 (UK) [hereinafter Online Safety Act]; Data Protection Act 2018, c. 12, § 123 (UK).

5: *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) (Austl.); on the speed of passage, *see generally* Senate Environment and Communications Legislation Committee, Parliament of Australia, *Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]*, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/SocialMediaMinimumAge (last visited Nov. 6, 2026) (recording the bill's referral on November 21, 2024 for report by November 26, with submissions closing on November 22 and "limited to 1-2 pages"); *id.*, Dissenting Report from Senator the Hon. Matt Canavan ¶¶ 1.1–1.3 (Nov. 2024), https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/SocialMediaMinimumAge/Report/Dissenting_Report_from_Senator_the_Hon_Matt_Canavan (describing the bill's passage as "not the Parliament's finest moment," and "forced through the Parliament with a haste not befitting its radical and unprecedented nature," with less than one week of public scrutiny and under 24 hours allowed for submissions).

these have broadly stumbled, as the Digital Services Act (DSA) has maximally harmonized this field, and the Court of Justice restricts abstract national rules against service providers in other Member States, curtailing much national action.[6] One online tracker, at the time of writing, records that at least 61 countries have engaged in discussion around some form of children's social media ban, with seven countries having implemented such a ban and four countries with bans awaiting enforcement.[7]

Likely wary of standing in the way of these political demands, in 2025, the European Commission announced a "special panel of experts on child safety online," with rapid meeting schedules and a varied roster of participants.[8] It quickly (in European Commission terms) proposed the EU KIDS Act (referred to as the Proposal or KIDS Act Proposal in this Article), to plug the gap.[9]

This Article argues that this Proposal is sloppy work that, if not withdrawn, significantly patched and reworked, will do real harm, regardless of whether one believes a social media prohibition or child-centered design obligations are good or bad policy ideas. The drafting leaves huge gaps, inconsistencies, surprises, omissions, and uncertainties. This brings consequences for adults and children alike across Europe and, through cascading regulatory effects, across the world.

The Article first, in Part I, digs into the broad mechanics of this complex Proposal to outline its function and how it would likely function in practice. It then looks, in Part II, at the specific regulated services, and highlights tensions within them. In the subsequent Parts, the Article then turns to a series of thematically grouped, cross-cutting issues in the Proposal and analyzes them in context, including unintended prohibitions, infrastructures of attestation and assurance, challenges caused by requiring tools for parents and guardians, and issues of monitoring. The Article then draws this together in a concluding section.

First, however, as a matter of introduction, the Proposal will be outlined. Already, a set-up of the Proposal will illustrate some initial warning signs, some of which will be elaborated on in detail throughout the remainder of the Article.

6: *See* Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, art. 28, 2022 O.J. (L 277) 1 (EU) [hereinafter Digital Services Act] (specifying, and thus maximally harmonizing, rules relating to children that apply to online platforms); Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on electronic commerce), art. 3(2), 2000 O.J. (L 178) 1 (EC) (limiting Members States' ability to regulate platforms in other Member States); *see also* Joined Cases C-188/24 and C-190/24, WebGroup Czech Republic and Coyote System, ECLI:EU:C:2026:492, ¶ 85 (June 16, 2026) (interpreting the E-Commerce Directive in regard to the limitation on regulation from other Member States); *see generally* Jessica Galissaire, Salma Gomez, & Lena-Maria Boswald, *Social Media Age Gating in the EU*, Interface (May 19, 2026), https://www.interface-eu.org/publications/social-media-age-gating-eu [https://perma.cc/ATK7-54XW] (tracking the interplay between these aspects and the EU social media ban discussions).

7: Ramsha Jahangir & Justin Hendrix, *Tracking Efforts To Restrict Or Ban Teens from Social Media Across the Globe*, Tech Pol'y Press (last updated Oct. 23, 2026), https://techpolicy.press/tracking-efforts-to-restrict-or-ban-teens-from-social-media-across-the-globe [https://perma.cc/YSV5-TJTD].

8: Eliza Gkritsi & Pieter Haeck, *Europe's Effort to Block Kids from Social Media Gathers Pace*, POLITICO (May 20, 2025), https://www.politico.eu/article/eu-children-social-media-regulation-platforms-big-tech/ (discussing the political demands of Member States); Jörg M. Fegert & Maria Melchior, *Child Safety Online: Protecting and Empowering Minors in a Digital World* 4 (July 13, 2026), https://commission.europa.eu/document/download/d833504d-5ec3-4fac-945f-38e7d0bd5326_en?filename=Special-panel-report.pdf (noting three meetings in just over a three-month period, containing varied participants each time).

9: *Commission 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 (Sept. 17, 2026), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0681 [https://perma.cc/G7GK-GXRA] [hereinafter KIDS Act Proposal].

A. ACCESS

The Proposal prohibits account creation and account-based access below age 15 for "online social networking services" (hereinafter "social networks" for convenience), such as Instagram, and "video-sharing platform services" (hereinafter "video platforms" for convenience), such as YouTube.[10] These definitions are drawn from the Digital Markets Act (DMA), a regulation that places *ex ante*, competition-flavored obligations on the largest technological gatekeepers.[11] The delayed account creation duties only apply to services exhibiting certain features that pose a "risk."[12] Yet the definition of risk is so broad that this narrowing does very little to reduce the scope of the law. A service is considered risky if it is designed, or has functionality, with the intention or reasonably foreseeable consequence of "incentivis[ing] interactions with the service or with content or other recipients of the service."[13] Commercial services broadly attempt to incentivize consumers to use them, meaning that the qualification of a risky service excludes almost nothing.

Such services may, optionally, allow guardians to set up accounts on behalf of 13- to 15-year-olds. Under the Proposal, these accounts are limited to a maximum daily usage time, per service, of one hour.[14] Where video platforms are specifically directed at children, they may allow children under 13 to access a specially designed version of their service through their guardian's account.[15] It is noteworthy that explicit age restrictions on account creation are *not* placed on other in-scope services, such as AI companions.

B. DESIGN

The Proposal places feature-level design obligations on social networks and video platforms, regardless of whether the features pose a risk that would bring the services within scope of the delayed account creation duties. These features include limiting addictive design, functionality of recommender systems, default settings, discoverability, and economic transactions.[16] The Proposal then selectively extends these provisions to the other in-scope services: AI systems (including companions and chatbots) and online games.[17] Many of these design provisions echo aspects of regimes in other jurisdictions, such as the UK's Online Safety Act and Age-Appropriate Design Code.[18]

Design obligations in the Proposal apply to any in-scope service that is "accessible to minors" (a test never defined).[19] These design obligations directly remove some of the main functionality relied upon by current advertising-funded services—removing implicit engagement signals, cross-

10: *KIDS Act Proposal*, *supra* note 9, art. 6.
11: Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), art. 2, 2022 O.J. (L 265) 1 (EU) [hereinafter Digital Markets Act].
12: *KIDS Act Proposal*, *supra* note 9, art. 6(1).
13: *Id.*
14: *Id.* art. 6(2)(b).
15: *Id.* art. 7.
16: *Id.* arts. 9–13.
17: *KIDS Act Proposal*, *supra* note 9, arts. 14–15.
18: Online Safety Act, *supra* note 4, §§ 11–13 (UK); Data Protection Act 2018, c. 12, § 123 (UK).
19: *KIDS Act Proposal*, *supra* note 9, art. 2(1).

service data connection, and "like" interaction counts.[20] Because of this, the obligations effectively force these services to age-gate their product, so that these features can continue to apply to their adult markets, or to withdraw from the European market entirely. As a result—and as will be shown throughout this Article—the design obligations generate a variety of *de facto* restrictions and implicit obligations, not all of which appear to be intended.

C. INFRASTRUCTURE

Various public sector infrastructural obligations arise from the Proposal. Obligations are placed on EU Member States to construct universally available digital mechanisms for a guardian to present an attestation of parental responsibility.[21] The European Commission is obliged to create an EU Age Verification Scheme, which is effectively a mechanism for certifying digital identity providers to provide technical solutions for age verification, with special connections to the European Digital Identity Wallet, the digital ID framework established through the EU's eIDAS Regulation.[22] The details of digital identity in Europe are an extremely controversial and technical area.[23] The Commission kicks important decisions about this infrastructure almost entirely into the future via implementing acts, and specifies very little about how this infrastructure would work in the Proposal.[24]

There is an obligation on operating systems—think Apple's iOS and Google's Android as the core addressees—to share age signals between applications and services (after obtaining consent of the user), in theory allowing users to verify on one app to a high standard, and have that signal carry over, with consent, to other services they use.[25] There is a further obligation on software app stores to undertake some form of age assessment of users, and to engage in complex and nationally specific software age rating for every purchase and install.[26]

D. SCOPE

1. Territorial Scope

The DSA tempers the territorial scope of its platform regulation through requiring a "substantial connection" to the Union.[27] The KIDS Act Proposal engages in no such tempering. The Proposal's

20: *KIDS Act Proposal*, *supra* note 9, arts. 10(2), 11 (assuming that "like" counts fall under this provision); *see generally* Christian Montag et al., *Addictive Features of Social Media/Messenger Platforms and Freemium Games against the Background of Psychological and Economic Theories*, 16 Int J Environ Res Public Health 2612 (2019) 8 (discussing the psychological elements and technical practices used by commercial services to prolong usage on those service in order to expose users to more advertising).

21: *Id.* art. 31.

22: Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, art. 5a, 2014 O.J. (L 257) 73, *as amended by* Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework, 2024 O.J. (L 2024/1183) 1 (EU) [hereinafter eIDAS Regulation].

23: *See, e.g.*, EDRi & epicenter.works, *eIDAS Policy Analysis*, (Jan. 25, 2022), https://epicenter.works/content/eidas-policy-analysis-english (discussing some of the most controversial and technical areas of this domain).

24: *KIDS Act Proposal*, *supra* note 9, art. 30(2).

25: *Id.* art. 29(6).

26: *Id.* art. 16(1)-(4).

27: Digital Services Act, *supra* note 6, art. 3(e).

territorial scope is instead determined solely on the basis of whether or not the entity "offer[s] [their] services to recipients . . . in the Union," or in the case of AI systems, whether or not a service has been "plac[ed] on the market or put[] into service . . . in the Union," following the scope of the EU AI Act.[28] The Proposal thus brings services into scope that lack a substantial number of European users and do not target their services toward the EU. This means that the EU risks geoblocking in relation to services that may have otherwise considered themselves out of scope of the DSA. The Proposal serves to further add confusion to the overlapping and differing coverage across European platform regulation.

2. "Accessible to Minors"

Only services "accessible to minors" are within scope of the Proposal.[29] Yet whether or not a service is "*accessible to minors*" is not an explicit test laid out in the law. In UK law, undertaking a similar test was considered such an analytically taxing affair that the Online Safety Act 2023 introduced a "children's access assessment," with extensive regulatory guidance designed to elaborate upon it.[30]

The only legislative gloss on this is not found in the Proposal at all, but in the recitals of the DSA, which outline a three-pronged test:

> An online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes.[31]

Applying this test, a service that is not aware of minors using it, prohibits them from doing so in its terms of service, and is not directed at or predominantly used by minors could argue that the Proposal does not apply to it. This would be an important exemption. But the test appears nowhere in the Proposal. It is situated in the recital of the DSA, and as a recital rather than an operative article, it is barely even part of the DSA. Recitals are hardly a good place to provide legal certainty around a difficult test. Furthermore, many of the services in the Proposal, such as online games or chatbots, are not the online platforms this recital definition specifically applies to. They may well not be in scope of the DSA at all, meaning that even if we were to accept a recital of the DSA as an acceptable location for an important definition of a test in an entirely different law, such services would have no reason to hunt for definitions there. Consequently, we can say very little with certainty about what "accessible to minors" means.

28: *KIDS Act Proposal*, *supra* note 9, art. 2(2)-(3); Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), art. 2(1)(a), 2024 O.J. (L 2024/1689) 1 (EU) [hereinafter AI Act].

29: *Id.* art. 2(1).

30: Online Safety Act, *supra* note 4, § 35; *see generally* Ofcom, *Children's Access Assessments Guidance* (Apr. 24, 2025), https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf (last visited Nov. 6, 2026) (elaborating on the nuances and complexities of such an assessment).

31: Digital Services Act, *supra* note 6, recital 71.

E. COMPLIANCE AND ENFORCEMENT

The Proposal grafts enforcement onto three existing regimes—the national and European levels of the DSA, the EU AI Act, and the national data protection authorities provided by the General Data Protection Regulation (GDPR).[32] Member States are also asked to legislate to give enforcement power to a regulator of their choice to enforce the Proposal in relation to online games.[33] For the most part, proposed maximum fines and powers are grafted onto the fines in those regimes;[34] however, the Proposal is silent about the details of how coordination might work in these contexts. The Proposal is also silent about the enforcement of any duties that relate to operating systems. In the current version, there are no penalties or procedures connected to operating systems allocated, and thus the provisions would be unenforceable by any regulator.

The Proposal is, however, clear about one thing: it states bluntly that "Member State authorities shall not take decisions which run counter to a decision adopted by the Commission under this [Proposal]." This is text drawn from the DMA. As applied to data protection authorities, however, this could be legally challenged as the Charter of Fundamental Rights arguably requires those authorities to be independent of everyone, including the Commission.[35] A further concern is that, where the Proposal's obligations overlap with data protection law, the Commission—an executive institution not an independent authority—would in effect decide whether personal data processing is lawful, leaving data protection authorities to implement its conclusions rather than

32: *KIDS Act Proposal*, *supra* note 9, art. 34; Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), ch. VI, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

33: *KIDS Act Proposal*, *supra* note 9, art. 34(5).

34: There are some exceptions; for example, the 6% potential fine for providers of AI companions and general conversational chatbots in the KIDS Act Proposal is higher than that in the EU AI Act. *Compare id.* art. 34(2) (subjecting providers of AI companions and general conversational chatbots to administrative fines under Article 99 of the AI Act of up to 6% of worldwide annual turnover where the provider acted intentionally or negligently), *with* AI Act, *supra* note 28, art. 99(4) (capping fines for breaches of most operator obligations, including providers' Article 50 transparency duties, at €15 million or 3% of worldwide annual turnover, whichever is higher). *But see id.* art. 99(3) (permitting fines of up to €35 million or 7% of worldwide annual turnover, whichever is higher, for engaging in prohibited AI practices under Article 5).

35: *KIDS Act Proposal*, *supra* note 9, art. 34(7); Digital Markets Act, *supra* note 11, art. 1(7); Charter of Fundamental Rights of the European Union art. 8(3), 2012 O.J. (C 326) 391. One of the logics for this is that the public sector is a significant regulated entity covered by data protection law; *see generally* Orla Lynskey, *The 'Europeanisation' of Data Protection Law*, 19 Cambridge Y.B. Eur. Legal Stud. 252, 255–60 (2017) (discussing the extent of "horizontal" and "vertical" independence of data protection authorities vis-à-vis both national influence and European institutions). Some of this depends on whether the Court of Justice would consider a KIDS Act decision by the Commission as akin to an adequacy decision. If so, the Court's case law suggests that data protection authorities are bound by it as an adequacy decision binds the Member States "and their organs, which include their independent supervisory authorities," and which therefore "cannot adopt measures contrary to that decision" unless the Court declares it invalid. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, ¶¶ 117–118 (July 16, 2020); Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶¶ 51–52 (Oct. 6, 2015). Yet the Court has also held that such a decision "cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities" so that those authorities must remain able to examine complaints "with complete independence" and to bring their doubts before national courts to raise to EU level. Facebook Ireland, ECLI:EU:C:2020:559, ¶¶ 119–120, 157; Schrems, ECLI:EU:C:2015:650, ¶¶ 53, 57, 65. This kind of analogy is in any event imperfect as an adequacy decision is itself a data protection measure, adopted under a data protection instrument rather than a decision under an entirely separated sectoral regime not passed under a treaty basis for a data protection law. *Cf.* Facebook Ireland, ECLI:EU:C:2020:559, ¶¶ 113–114, 146 (holding that the Commission's standard contractual clauses decision did not prevent supervisory authorities from suspending or prohibiting transfers under Article 58(2) GDPR).

reach their own.[36]

II. SPECIFIC SERVICES

The KIDS Act Proposal covers many different services. In order to do so, it inherits definitions from other areas of EU law for some services and creates new definitions for others. Both approaches have significant, apparently unintended, effects on services that on their face might not appear to be in scope of the Proposal. Furthermore, the obligations placed on many of these services—especially in combination with the often very wide scope—have significant effects, leaving several major existing products in the market effectively unviable. These obligations also, in many cases, introduce a *de facto* age-gating requirement on accounts even where the service is not a social network or video platform.

This Article will now look at these services in turn, comment on some of these tensions, and following that, consider some further thematically grouped issues that apply across different services.

A. ONLINE SOCIAL NETWORKING AND VIDEO SHARING PLATFORM SERVICES

As mentioned previously, unlike the obligations for other services, those for social networks and video platforms attach to creating and having an account, which is justified by how, "typically," the features the Commission considers risky, such as recommender systems, are only made available to users with such accounts.[37] Minors' access to social networks and video platforms through accounts is staggered by age. Before age 13, only video platforms may offer access, and only as a profile within a guardian's account. From age 13 until age 15, both social networks and video platforms may offer access, but only with a guardian's consent and as part of that guardian's account. From age 15, minors may hold accounts freely and independently. A series of articles also mandates "safety-by-design" safeguards and protective measures for minors of all ages. Even those aged 15 and older, who can create their own accounts, will therefore have an online experience different from that of adults.

These "safety-by-design" provisions are specifically only scoped to social networks and video platforms but, in a flourish of bad drafting, the Commission constantly cross-references to and

36: *KIDS Act Proposal*, *supra* note 9, arts. 27–29, 34(6)–(7); Consolidated Version of the Treaty on the Functioning of the European Union, *supra* note 143, art. 16(2) (compliance "shall be subject to the control of independent authorities"); Case C-518/07, Comm'n v. Germany, ECLI:EU:C:2010:125, ¶ 36 (Mar. 9, 2010) ("mere risk" of political influence suffices to breach independence); Facebook Ireland, ECLI:EU:C:2020:559, ¶ 119 (Commission decision "cannot eliminate or reduce" supervisory authorities' Charter powers). *Compare* Case C-97/23 P, WhatsApp Ireland Ltd. v. Eur. Data Prot. Bd., ECLI:EU:C:2026:81, ¶ 102 (Feb. 10, 2026) (noting that the European Data Protection Board, which unlike the Commission is an independent body, "unconditionally binds" supervisory authorities), *with KIDS Act Proposal*, *supra* note 9, art. 34(7). The Commission's original GDPR proposal sought similar powers to suspend and overrule supervisory authorities. These did not survive into the final text. *See* Lynskey, *supra* note 35, at 278; GDPR, *supra* note 32, arts. 63-66.

37: *KIDS Act Proposal*, *supra* note 9, recital 21.

applies such obligations to other services, even where this makes little sense.[38] It does so in almost all situations without specifying that they apply *mutatis mutandis*.[39]

1. These Aren't the Platforms You're Looking For

The definitions of social networks, video platforms, software application store, and operating system all draw from the DMA. The structural form of the DMA is to have extremely broad foundational definitional scope, as the obligations only apply to a tiny subset of the very largest actors designated explicitly as gatekeepers within that scope. The purpose of this scope is fundamentally in tension with a law designed to impose horizontal obligations on all in-scope actors. Furthermore, while the DSA carries an "ancillary feature" exemption, designed to exempt things like online comment sections that incidentally would otherwise meet the definition of "online platform," no parallel exemption applies to social networks and video platforms in the Proposal.[40] The Proposal explicitly deems both as "online platforms" in all cases.[41]

The very different logic of its inherited material scope means that many services that make little sense to regulate fall within the Proposal's scope. These would include:

- a corporate collaboration or messaging service such as Slack, which a 14-year-old intern is using—it can be used to message anyone in an organization, or, as is often the case with services such as Microsoft Teams, in other organizations;
- a music streaming service such as Spotify, which allows musicians to upload music videos alongside songs, allows users to upload video podcasts, and lets people share recommendations with each other—it has features designed to promote its use, as well as recommender systems, in-app messaging, and podcast comments;
- a book recommendation and review service such as Goodreads where users can post reviews and comments visible to any other user, and, unlike under the DSA, there is no ancillary feature escape route;
- a gaming service such as Chess.com, used by competitive school chess clubs—it has forum and chat services, and as a core feature, connects players who do not otherwise know each other.

It does not seem proportionate to restrict an intern, a music-listener, a book-seeker, or a competitive chess player to a maximum of one hour of use per day, but none of them are obviously exempted from the Proposal.

38: *See KIDS Act Proposal*, *supra* note 9, art. 14(1)(a)–(c) (applying Articles 9, 11 and 13 to AI companions and general conversational chatbots, including rules on account recommendations, contact synchronization and the age-15 threshold for changing default settings); *id.* art. 15(1)(a)–(c) (applying parts of Articles 9, 11 and 12 to online games, although Article 9(1) is expressly limited to social networks and video platforms); *id.* art. 20(4)(a)–(b) (requiring guardian tools for all covered services to manage settings "pursuant to Articles 11 and 12" and time limits under provisions that concern settings rather than time limits).

39: *Compare id.* art. 5(1), (3) (applying DSA provisions "mutatis mutandis"), *with id.* arts. 14(1), 15(1) (omitting that qualifier).

40: *Compare* DSA, *supra* note 6, art. 3(i) & recital 13 (exempting from "online platform" services whose public dissemination is a minor and purely ancillary feature, such as a newspaper comments section), *with KIDS Act Proposal*, *supra* note 9, art. 3(2) (deeming online social networking services, video-sharing platform services and software application stores "online platform[s]" under DSA art. 3(i)).

41: *Id.* art. 3(2).

2. Escaping the Scope

Some of these bans might be overcome by stripping certain features. Goodreads could disable any personalized recommendations—although it should be queried whether we want to pass legislation that makes it less compelling for children to read books. But for other services, avoiding the Proposal's scope is much harder. Spotify would effectively have to remove music videos and video podcasts, and any music recommendations based on listening habits, all an intrinsic part of its product and, again, of limited apparent risk. No one appears to be concerned about children listening to too many personalized music playlists. Chess.com would have to remove the ability to play a stranger, which is really the whole point of an online chess game. Slack or Microsoft Teams would have to remove their inherent ability to chat or join meetings with participants outside of one's organization. This may work for school-provided versions, but not for enterprise customers.[42]

There are, however, reasons that community-hosted platforms, such as Mastodon or other "Fediverse" social network instances, may fall out of scope, even where these are used by children. The Commission may not have anticipated this. It is not possible to qualify as an information society service if a service is not "normally provided for remuneration," and an information society service "must represent an economic activity."[43] Mastodon instances are typically community-organized and donation-funded, and have no functionality for advertising. That being said, one consequence of this interpretation is that such services would not receive intermediary liability protection in European law, needing to rely instead on relevant defenses in national law relating to any liability they are accused of bearing. It should also be noted that the Commission has designated Wikipedia, a large, ad-free, donation-run platform, as a very large online platform under the Digital Services Act, and that this is a live area of cross-cutting legal contention.[44]

B. ONLINE GAMES

The definition of online games is perhaps the most baffling in the entire Proposal, and brings significant regulatory consequences. It firstly includes many games that do not appear to meet the normal definition of "online." It secondly includes many *de facto* social networks, without being clear on whether this prohibition precludes games from also qualifying as social networks separately. Finally, despite all the noise about banning loot boxes in games, the Proposal appears to, somehow—and inexplicably—forget to do this, instead only banning them for select other in-scope services.

42: Slack or Microsoft Teams could also make a more complex argument that the messaging part of their service should be analyzed separately as a number-independent interpersonal communications service, outside the KIDS Act Proposal, which could disqualify the rest of the service as it takes away the core criteria. They might do this following the logic of the General Court in separating Meta's Messenger out as a separate core platform service under the DMA. *See* Case T-1078/23, Meta Platforms v. Comm'n, ECLI:EU:T:2026:357, ¶ 95 (June 3, 2026).

43: Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying Down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services, 1(1)(b), 2015 O.J. (L 241) 1 (EU) [hereinafter Single Market Transparency Directive]; Case C-484/14, McFadden v. Sony Music Ent. Germany GmbH, ECLI:EU:C:2016:689, ¶ 40 (Sept. 15, 2016).

44: Commission Decision of 25 April 2023 Designating Wikipedia as a Very Large Online Platform in Accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council, C (2023) 2742 final (Apr. 25, 2023). It seems likely that Wikipedia would not want to contest foundationally being an information society service, as its liability shielding is likely extremely valuable to it in a way that it may not be for a small Mastodon instance.

1. Online Games Include All Offline Games?

The definitional scope of "online games" includes many games that are functionally not online games.[45] The definition includes "video game[s]," which are information society services "that allow[] the recipients of the service to engage, by means of application accessed locally or remotely, including through the use of a durable medium and that involves interaction with a user interface or input device to generate visual feedback from a display device in a simulated environment for play or entertainment purposes."[46] It also includes "video gaming platform[s]," which are online platforms "that [involve] interaction with a user interface or input device to generate visual feedback from a display device in a simulated environment [for play or entertainment purposes]."[47]

The recitals make an extremely odd and difficult-to-justify distinction between in-scope and out-of-scope games. It effectively hinges on whether a game is or is not downloadable.[48] It does not hinge on whether the video game has online connectivity or features, and no exemptions exist in the Act for non-online games that are open source, made by individuals, or even by other children. This effectively means, as currently written, that no downloadable game software, even if played offline, can enable the camera, microphone, geolocation, or push notifications during core school hours and sleep time without checking whether the user is at least 15; this will be a challenge given that the game is offline.[49] It also means that such games must provide guardians with tools to control use that are not easily circumvented. This effectively requires a separate "admin" authentication layer on all offline downloadable games, like a secret control panel that only a parent has the passkey for.

Given the lack of exemptions, this law would apply to all games that have *ever* been downloadable online. For example, the whole of the Internet Archive's Classic PC Games archive, or the My Abandonware archive of abandoned historic computer games, would need to provide guardian tools.[50]

There is uncertainty around whether the Proposal would create liability for resellers of physical games now also available online. The recital seems to suggest only games "exclusively" available physically are exempted.[51] But, for example, classic, unsafeguarded Nintendo Game Boy cartridges, such as the *Pokémon Trading Card Game*, are not "exclusively" available through physical media, but *also* downloadable legitimately through the Nintendo Switch's "classics" collection .[52] Given most physical media is read-only, full enforcement of the law would turn much of the history of video gaming into e-waste. Resellers do have an argument they can run, as the Commission appears to

45: *KIDS Act Proposal*, *supra* note 9, art. 3(5)(e).
46: *Id.*, art. 3(5)(e)–(f).
47: Note that the square brackets are in the original; this appears to be an unfinished remnant of drafting that has not been removed before publication. *Id.*, art. 3(5)(e)–(g).
48: *See id.* recital 12.
49: *Id.* art. 15(1)(b) (instructing the application of art. 11(1)). Article 11(1) appears inseparable from Article 11(2), *see id.* art. 11(2), unless it is truly intended that online games can just have the user disable these default settings, which makes them quite ineffective protections (as these features are typically already mostly disabled by the operating system by default).
50: *See, e.g.*, *Classic PC Games*, Internet Archive, https://archive.org/details/classicpcgames [https://perma.cc/R7FK-MLL7] (last visited Oct. 23, 2026); My Abandonware, https://www.myabandonware.com/ [https://perma.cc/YV92-XMCQ] (last visited Oct. 23, 2026). There is an exemption for "educational" and "scientific" repositories, but these are archiving services, which usually have a separate classification in European law alongside "educational" or "scientific."
51: *KIDS Act Proposal*, *supra* note 9, recital 12.
52: Nintendo, *Game Boy – Nintendo Classics*, https://www.nintendo.com/en-gb/Games/Nintendo-Switch-download-software/Game-Boy-Nintendo-Classics-2339836.html (last visited Nov. 6, 2026).

have misinterpreted EU law concerning digital services in the recitals of the Proposal. The test cannot be whether a game is "exclusively" available offline. This is because any game purchased in physical media without an online component cannot qualify as an "information society service," and therefore cannot fall within the scope of the definition, or even get to the point of being tested.[53] In EU law, recitals should not contradict the articles, particularly at the proposal stage, before any political trading.[54] The recitals should set out concise reasons for the chief provisions of the enacting terms, without either reproducing them or adding further normative provisions.[55] Here, they fail to do that.

Other than old physical games, there is the long tail of anything downloadable that could be considered a video game, from the New York Times crossword to the legendary 40-year-old open-source *NetHack*, a still regularly updated roguelike played entirely in a computer terminal. It could be argued that a crossword is not a "simulated environment," and should thus fall outside of the definition, but this test seems shaky and tenuous.[56] It could also be argued that a community-developed, open-source game is not an information society service, similar to a Mastodon instance, as argued above. These interpretations are far from straightforward to argue and apply.

The draft should be amended to carve out video games that have no online features allowing interaction with other users as part of gameplay, and have no in-game purchases, subscriptions, or advertising-funded features that confer customization or advantage. It should exempt online updates, backups of saves, leaderboards, expansion packs, and similar features, as all of these relate to either harmless features, important security provisions that should not be disincentivized, or simple distribution. Offline games distributed on physical media should be exempt in all situations.

2. Social Networks in Trenchcoats

Only the social network and video platform categories face a staggered prohibition. The definitional boundary between these categories and others is therefore hugely important to regulatees. Online games aimed at kids, like *Roblox* and *Fortnite*, would lose an enormous chunk of revenue if considered social networks: kids would be prohibited until age 13 and given one-hour time limits until age 15. Yet, as online games, they need only provide some safeguards and tools for guardians. Which are they?

The Proposal creates a deeming rule in its recitals that "where an online game also has certain features corresponding to a video sharing platform, it shall be considered an online game for the purpose of this [Proposal]."[57] It does not specify whether this deeming logic should be extended to social network-like games too. The Proposal also does not specify whether this deeming rule is

53: Single Market Transparency Directive, *supra* note 43, art. 1(1)(b)(ii), Annex 1, point 2.
54: *See* Maarten den Heijer, Teun van Os van den Abeelen & Antanina Maslyka, *On the Use and Misuse of Recitals in European Union Law* 10–13 (Amsterdam L. Sch. Legal Stud. Rsch. Paper No. 2019-31, 2019), https://ssrn.com/abstract=3445372 (finding that norm-setting and paraphrasing recitals more than double between Commission proposal and adopted text, and documenting recitals' use as a vehicle for negotiated compromise); *see generally* Tadas Klimas & Jurate Vaiciukaite, *The Law of Recitals in European Community Legislation*, 15 ILSA J. Int'l & Comp. L. 61 (2008); *cf.* Case C-134/08, Hauptzollamt Bremen v. J.E. Tyson Parketthandel GmbH, ECLI:EU:C:2009:229, ¶¶ 15–19 (Apr. 2, 2009); Joined Cases C-154/04 & C-155/04, Alliance for Nat. Health v. Sec'y of State for Health, ECLI:EU:C:2005:199, ¶¶ 71–75 (Apr. 5, 2005) (Opinion of Advocate General Geelhoed).
55: Interinstitutional Agreement of 22 December 1998 on Common Guidelines for the Quality of Drafting of Community Legislation, pt. 10, 1999 O.J. (C 73) 1.
56: *KIDS Act Proposal*, *supra* note 9, art. 3(5)(f).
57: *Id.* recital 12.

an "also", or if instead being considered as an online game under the Proposal forecloses the regime from considering it as a social network. If passed as is, we can expect lengthy legal contestation as social networks (further) gamify themselves in order to attempt to fall out of any age-gating. Virtual worlds, unsuccessfully branded as "metaverses," are particularly difficult to classify in this regard.

3. Loot Boxes Banned in All Services Except Games

One area of online games that has been especially salient in policy spaces around the world in recent years is the "loot box."[58] Loot boxes are in-game purchases with an outcome determined by chance, not dissimilar to packets of trading cards. Their prevalence has raised concerns about similar psychological and financial harms associated with gambling. While the recitals of the law specify that the Proposal includes measures "preventing minors from being exposed to loot boxes" and, in games, variable reward systems associated with gambling-related and compulsive behaviours, astoundingly, the corresponding obligation in the operative text to prevent minors from being exposed to variable reward systems does not apply to online games, only to social networks, video platforms, AI companions, and chatbots.[59]

C. AI SYSTEMS

AI systems have two subcategories in the Proposal: general conversational chatbots and AI companions. Both are new concepts in EU law. Both utilize definitions from the EU AI Act. Neither is subject to an age ban—the KIDS Act Proposal blesses AI usage with no minimum age, subject to these providers putting in place protective measures for minors. Even though there is no minimum age for use, age verification is, in practice, mandated for these providers, because they have an obligation to prohibit children under 13 to open an account other than through a guardian.[60] Below, two main issues are analysed: the exemption of educational chatbots from the regime (and the difficulty in drawing the line based on such functionality), and the difficulty in marketing a companion that does not engender emotional dependence in any child.

1. Exempting Educational Chatbots

General conversational chatbots mean "a general-purpose AI system with general conversational functionalities for direct interaction with users that is capable of providing assistance across multiple domains and tasks."[61] Exempted from this definition are "AI systems whose conversational functionality is limited to a specialised service, task or pre-defined set of functions, including specialised customer-service, business operation, technical-support, transactional, educational, information-retrieval, industrial or manufacturing AI applications."[62] The definition is specifically

58: *See generally* John Woodhouse, *Loot Boxes in Video Games*, House Commons Libr. (Aug. 13, 2024), https://researchbriefings.files.parliament.uk/documents/CBP-8498/CBP-8498.pdf [https://perma.cc/5L9C-9LRR] (describing the saga of loot boxes being considered in parliament, by regulators and Government to date).
59: *KIDS Act Proposal*, *supra* note 9, art. 13(2), recitals 31, 40.
60: *Id.* art. 14(1)(d).
61: *Id.* art. 3(5)(d).
62: *Id.* art. 3(5)(d).

designed to keep out some narrow uses while clearly including the major user-facing services like OpenAI's ChatGPT and Anthropic's Claude.

First, it is not clear why an educational chatbot should be excluded from scope, given that such chatbots are disproportionately likely to be aimed specifically at children as a customer base. What makes a chatbot "educational" is unspecified, and likely to be subject to significant legal contestation. While the Proposal's entire scope excludes services "designed for primarily educational purposes" which are also operated by educational establishments, or on their behalf,[63] the educational exemption relating to "general conversational chatbots" lacks the "operated by" or "on behalf of" limb of this test, which is the one that makes the whole test actionable even though underspecified. This has been a pervasive problem in software, as researchers have assessed the majority of popular "educational" apps targeted at children as being of lower educational quality.[64]

The definition further trips up on what it means to be "limited." Is this a technical limitation, put in place by content moderation guardrails; a capability limitation, trained in; an intentional limitation, bound by contract or similar? A mixture of all of these? It is a regular occurrence for individuals to "jailbreak" limited-purpose chatbots (such as those in customer service) for uses beyond their intended function. Typically this can be assessed through either looking at the intent, the realized use, or the potential use of a system. However, the Proposal does not hint at which one of these conceptual categories it refers to.[65] Without such clarity, the test is effectively impossible to operationalize.

2. Inherently Dependable Companions

The definition of companion appears to immediately be at tension with the obligations around companions. While the definition includes any AI systems "[provide] sustained, personalised interaction or companionship which simulates or facilitates a social, emotional or interpersonal relationship," design obligations concerning on AI companions require "avoiding design features and system behaviours that simulate interpersonal relations that are likely to create emotional dependencies."[66] It is not stated in whom these features or behaviors are supposed to be "likely" to engender these dependencies in. This is a challenge, as literature appears to indicate that adolescents with mental health problems are more predisposed to developing dependency on such AI tools.[67] Does the existence of this very common subset of minors for whom emotional dependencies appear a side-effect of companion usage in general mean that it will be very hard to market any companion at all under the regime? Again, the actual impact of the Proposal on the

63: *Id.* art. 2(4)(c).

64: *See generally* Marisa Meyer, Jennifer M. Zosh, Caroline McLaren, Michael Robb, Harlan McCafferty, Roberta Michnick Golinkoff, Kathy Hirsh-Pasek, & Jenny Radesky, *How Educational Are "Educational" Apps for Young Children? App Store Content Analysis Using the Four Pillars of Learning Framework*, 15 J. Child. & Media 526 (2021), https://doi.org/10.1080/17482798.2021.1882516 (finding that, of the top 100 apps in mobile app stores and 24 apps most commonly played by children in a longitudinal cohort study, 58% were of low educational quality).

65: *See KIDS Act Proposal*, *supra* note 9, art. 3(5)(d); Robert Gorwa & Michael Veale, *Moderating Model Marketplaces: Platform Governance Puzzles for AI Intermediaries*, 16 L. Innovation & Tech. 341, 345-46 (2024).

66: *KIDS Act Proposal*, *supra* note 9, arts. 3(5)(c), 14(1)(a).

67: *See, e.g.*, Shunsen Huang et al., *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*, 17 Psychol Res Behav Manag 1087, 1087 (2024) (noting in a two-wave longitudinal study of 3,843 Chinese adolescents that mental health problems positively predicted subsequent AI dependence).

legality of products is left to the inability to square a complex circle, rather than a prohibition on the face of the law.

D. SOFTWARE APPLICATION STORES

The scope of "software application store" is also very broad, again as it originated in the DMA. Its definition there is "a type of online intermediation service, which is focused on software applications as the intermediated product or service."[68] Software applications are defined as "any digital product or service that runs on an operating system," and an operating system is "system software that controls the basic functions of the hardware or software and enables software applications to run on it."[69] This definition of "software application store" creates some immediate scope questions.

1. Shared Devices

While the Commission may have been envisaging mobile phones when considering a regime to control software applications, the Proposal gives seemingly no thought to shared devices. Researchers have indicated that shared devices are much more common than people believe and have found that users' own reporting of device sharing was unreliable; when users kept diaries of their usage, they often expressed surprise at just how much they shared and used shared devices.[70]

The prototypical shared device featuring an app store is a family television. As anyone purchasing a television in recent years knows, it is almost impossible to buy one that does not have a microphone and a strong tendency to demand an internet connection. Accounts on these TVs, such as to purchase apps, are typically shared across the family rather than individualized, even if viewer profiles or similar features may exist within an account on a streaming service. Users typically mediate this sharing through social etiquette rather than through technical controls or division.[71] Who exactly is the "recipient" of a downloaded app on an app store on a shared device?[72] How is age assurance supposed to exclude children, unless shared accounts are simply prohibited? In any case, this would be a massive change that is very unlikely to be easily retrofitted, given how many TVs no longer receive software updates. Many TVs simply do not contain the technology that would make any reasonable type of age assurance possible. A similar, and perhaps more daunting, challenge concerns app stores in automobiles, where rear-seat screens make such stores accessible to minors on the adult's account which relates to the entire car, and thus brings such car apps within scope of the obligations.

68: Digital Markets Act, *supra* note 11, art. 2(14).
69: Id., art. 2(10), (15).
70: Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, Sunny Consolvo, *"She'll Just Grab Any Device That's Closer": A Study of Everyday Device & Account Sharing in Households*, *in* Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems 5921, 5930 (2016), https://doi.org/10.1145/2858036.2858051.
71: *See generally* Ji Eun Song, Jaeyoun You & Joonseek Lee, *"I Might Be Using His… But It Is Also Mine!": Ownership and Control in Accounts Designed for Sharing*, *in* Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems 1 (2021) https://doi.org/10.1145/3411764.3445301 (describing how users navigate shared accounts socially and technically).
72: *KIDS Act Proposal*, *supra* note 9, art. 16(4).

2. What's in Store? Who Cares?

Unlike the social network and video platform scope, there is no condition of "risk" to mitigate the enormous scope of the DMA app store definition.[73] This appears to bring into scope low-risk services, such as browser add-on stores and the Amazon Alexa "skills" store, neither of which is easy to imagine posing a harm to a child. Given the small number of app stores, a designation regime, rather than a regime scoped by definition and regulatee self-assessment alone, might be more appropriate.

Some app stores that appear to pose no risk to children may escape the Proposal, but not because the Proposal or its recitals say so. Any exemption must instead be pieced together from the definitions the Proposal borrows from other instruments. Corporate software stores seem to escape because under the Platform-to-Business (P2B) Regulation, which supplies the constituent definition of "online intermediation services," users are not consumers, but employees.[74] Certain volunteer-run app stores, such as F-Droid, which provides free software for "de-Googlified" versions of Android, also would appear to fall out due to this definition, as they do not support transactions (all software must be free) and no stage of their upload process involves creating a contract with them as an intermediary.[75] These are quite arcane ways to exempt services, and both would likely require legal advice to understand.

3. An Accidental Book Ban?

Some operating systems directly run types of digital products that differ from what one might usually consider a software application. Consider an e-ink Amazon Kindle, which is an e-book reader where all functionality is included in the device, which has a locked-down operating system that facilitates the only permitted way to access or use digital products or services. Given that "software applications" are defined as "any digital product or service that runs on an operating system," that e-books clearly are a digital product (if not the prototypical one), and that they run directly on the Kindle operating system, this provision would appear to require an age-rating

73: *See* discussion *supra* Section I.A.

74: Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services, art. 2(2)(b), 2019 O.J. (L 186) 57 (EU) [hereinafter P2B Regulation, as it is known due to regulating platform-to-business relations]. They may also not be accessible to minors depending on, for example, who the firm employs.

75: *Id.* art. 2(2)(b)–(c). *See About*, F-Droid, https://f-droid.org/en/about/ (last visited Nov. 6, 2026) (describing F-Droid as "made by volunteers who care about free and open software"); *Inclusion Policy*, F-Droid, https://f-droid.org/en/docs/Inclusion_Policy/ (last visited Nov. 6, 2026) (requiring all apps to be free software and barring dependencies on Google Play Services); *see generally Submitting to F-Droid Quick Start Guide*, F-Droid https://f-droid.org/docs/Submitting_to_F-Droid_Quick_Start_Guide/ [https://perma.cc/S2HR-V3JC] (last visited Oct. 27, 2026) (describing F-Droid's submission process, which contains no contractual step nor terms, with F-Droid deriving the right to publish entirely from the open license of the app, meaning, as the site explains, that the uploader need not even be the author of the app).

system to be created for all books sold digitally by Amazon.[76] As books do not carry age ratings, this would be an enormous endeavor. Restricting kids' access to books on the basis of spurious age rating has significant fundamental rights consequences for both children and authors, and it is not acceptable that drafting could accidentally lead to this type of conclusion.[77] It is possible to argue that the Kindle should be excluded. Perhaps books do not "run" on an operating system and are therefore not executable, although recent versions of the .epub open book standard include scripting.[78] Perhaps the Court of Justice will maintain, as it has in reference to a different regime, that "an e-book is not a computer program."[79] Perhaps Amazon is not an intermediary of e-books, but a reseller, which changes the definitional flow.[80] However, all this is a lot of uncertainty for a law that should be drafted so as to ensure it unambiguously does not require the age-rating of books. A designation-based regime would provide much clearer legal certainty, even with the current set of definitions.

III. WHEN A SETTING BECOMES A BAN

Article 11 on "safe settings" is deeply confusing to apply. Its premise is that for all minors, in-scope services should not turn on geolocation, tracking features, access to microphones or cameras, recommendations of accounts, synchronization of contacts, push notifications, and AI memory, by default.[81] It then goes on to state that such "default settings" may "only be changed by the provider" where the user is over 15 and has consented to this, but in any case, tracking and geolocation should be turned off after each session.[82]

It is not clear what it means for a provider to change the default setting for those over 15 with consent. A default setting is one that is there when you first use a service. If you have to consent to change a default setting, then what makes this different from changing an actual setting?

It could be that Article 11 simply prohibits nudging for users under age 15. This means that minors must not be guided by the platform to enable these settings, such as through notifications

76: DMA, *supra* note 11, art. 2(15); *see KIDS Act Proposal*, *supra* note 9, art. 3(2), (4) (adopting the DMA's definitions of "software application store" and "operating system"); *id.* art. 16(1) (requiring an age-rating system that "shall apply to each software application offered on the software application store"). On the Kindle, *see* Amazon.com, *Kindle Store Terms of Use* § 1 (Oct. 21, 2026), https://www.amazon.com/gp/help/customer/display.html?nodeId=201014950 (licensing Kindle Content, including content from third-party providers, for use "solely through Kindle Software" on supported devices, including Kindle e-readers); Brad Linder, *WinterBreak Tool Can Jailbreak Most Recent Kindle Hardware*, Liliputing (Jan. 2, 2025), https://liliputing.com/winterbreak-tool-can-jailbreak-most-recent-kindle-hardware/ (describing Kindle e-readers as running a custom Linux distribution locked to Amazon's ecosystem, on which third-party software can be installed only by jailbreaking).

77: *See, e.g.*, Alison Flood, *Children's Minister Raises Doubts over Age-Banding*, Guardian (Sept. 12, 2008), https://www.theguardian.com/books/2008/sep/12/ed.balls.age.guidance.publishers.association [https://perma.cc/4V7C-HWYU] (noting 77% of authors opposed previous age-banding plans for books, and publishers expressed that it would be "almost inconceivable" for banding to be placed on books without an author's approval).

78: *EPUB 3 Overview* (Mar. 13, 2025), World Wide Web Consortium, https://www.w3.org/TR/epub-overview-33/ [https://perma.cc/B5QP-784C].

79: Case C-263/18, Nederlands Uitgeversverbond v. Tom Kabinet Internet BV, ECLI:EU:C:2019:1111, ¶ 54 (Dec. 19, 2019).

80: *See* P2B Regulation, *supra* note 74.

81: *KIDS Act Proposal*, *supra* note 9, arts. 11(1), 14(1)(b).

82: *Id.* art. 11(2).

or promises of better functionality.[83] They certainly should not be enabled by default, although the actual value of such a prohibition is limited given that most of the above settings are already gatekept by mobile operating systems, which require apps to receive a user signal before enabling them.[84] For example, it is not possible, on modern iOS or Android, for an app to enable geolocation, microphone, camera, or push notifications, without an active step by the user.[85]

The problem with this reading comes from the statement that "[d]efault settings referred to in paragraph 1 may only be changed by the provider where the minor is above the age of 15 years and was clearly and unambiguously informed about such changes and has explicitly consented to such changes."[86] What does this mean? Default settings might be read literally as the default value of a setting (*i.e.*, on or off), but they might also simply refer to the settings themselves, such as camera and geolocation, by means of giving them a moniker—a common verbal tic of EU law.[87] If "default settings" refers to actual defaults, then this really makes no sense, as it is impossible for a user to change a default setting. Default settings are set by the designer; users change them from the starting position of this default. Instead, there is support for the idea that "default settings" is supposed to mean "settings" from the next sentence, which states that "[d]efault settings referred to in paragraph 1 point (a), where enabled by minors, shall be turned off after their session on the service ends."[88] This sentence seems to mean instead that *settings* referred to in 1(a) (geolocation and tracking) should be returned to a default of "off," regardless of the minor's choice, after a session ends.

Based on this interpretation, we would need to read Article 11(2) as, "the above settings may only be changed by the provider where the minor is above the age of 15 and has consented." It

83: *Id.* recitals 18, 41 ("minors should not be requested to lower the level of sensitive settings during account creation, such as access to geolocation or camera," and "providers should not repeatedly prompt or entice minors to lower their level of protection").
84: *See* Android Developers, *Request Runtime Permissions*, https://developer.android.com/training/permissions/requesting (last visited Nov. 6, 2026) (requiring apps on Android 6.0 and later to request "dangerous" permissions at runtime through a system dialog the app cannot customise); Apple Inc., *Requesting Authorization to Capture and Save Media*, Apple Developer Documentation, https://developer.apple.com/documentation/avfoundation/requesting-authorization-to-capture-and-save-media (last visited Nov. 6, 2026) (stating that "the user must explicitly grant permission for each app to access the camera and microphone").
85: *See* Apple Inc., *Requesting Authorization to Use Location Services*, Apple Developer Documentation, https://developer.apple.com/documentation/corelocation/requesting-authorization-to-use-location-services (last visited Nov. 6, 2026) (system alert asking the user to grant or deny location access); Apple Inc., *Requesting Authorization to Capture and Save Media*, *supra* note 84 (camera and microphone); Apple Inc., *Asking Permission to Use Notifications*, Apple Developer Documentation, https://developer.apple.com/documentation/usernotifications/asking-permission-to-use-notifications (last visited Nov. 6, 2026) (system prompt to allow or deny notifications); Android Developers, *Request Runtime Permissions*, *supra* note 84 (location, camera and microphone); Android Developers, *Notification Runtime Permission*, https://developer.android.com/develop/ui/views/notifications/notification-permission (last visited Nov. 6, 2026) (notifications off by default for apps newly installed on Android 13 and later until the user grants permission). *But see* Apple Inc., *Asking Permission to Use Notifications*, *supra* (allowing iOS apps to obtain "provisional" authorization that is granted automatically without prompting the user, with notifications delivered quietly to the notification centre only).
86: *Id.* art. 11(2).
87: *See, e.g.*, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, art. 6(4), (6), 2011 O.J. (L 304) 64 (EU) (calling the pre-contractual information listed in art. 6(1) the "information requirements"); GDPR, *supra* note 32, art. 46(2)–(3) (providing that "[t]he appropriate safeguards referred to in paragraph 1" may be supplied by listed instruments, including standard contractual clauses); *cf.* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 132–33 (July 16, 2020) (holding that standard contractual clauses may, despite being described as an "appropriate" safeguard in a list called "appropriate safeguards", nonetheless in fact require supplementary measures to actually qualify as "appropriate" substantively).
88: *Id.*

would mean that all references to minors changing settings were to minors for whom such setting changes were permitted, such as those over 15. The recitals provide some support for this, giving examples of how, to have a "public [account]" or "host livestream [*sic*]," one should both require a minimum age and explicit consent from a guardian.[89] The vague obligation in Article 20 for providers to include, for guardians, "mechanisms aimed at managing settings pursuant to Articles 11 and 12," in combination with the previous prohibition in Article 11, leaves confusion as to whether a guardian is even permitted to turn on, for example, cameras on a social network for an under-15 or not.[90]

If Article 11 is to be read as a prohibition, then a whole lot of services that rely on these settings as core parts of their functionality become *de facto* prohibited. Strava, a running app with sharing and commenting features that bring it within scope of the social network provision, inherently requires geolocation to function. Insofar as exercise may help children spend less time on screens, this may seem a little like an own goal. Games that use a camera or microphone, such as augmented reality games, those that interact with physical toys, or those that have voice interfaces, are also prohibited for children under 15. The same goes for geolocation, which means the end of children under 15 playing Pokémon Go.[91] The reader can decide whether that is a good thing or not. AI firms will need to disable their memory function by default unless users verify they are over 15.[92] It also follows that no users in the EU can use voice-assisted AI, or AI that integrates directly with a camera, without age verification. Mainstream products that rely on these modalities, such as Amazon's Alexa or Meta and Ray-Ban's controversial "smart" glasses, are prohibited from functioning before an age verification process has taken place to ensure the user is over 15.

Many toys themselves may fall under a prohibition. AI companion means "an AI system, including a general-purpose AI system, that provides sustained, personalised interaction or companionship which simulates or facilitates a social, emotional or interpersonal relationship with a user."[93] Given that this definition anchors on the EU AI Act's much wider "AI system" definition, rather than its narrower subset definition of a "general-purpose AI system", and also contains the wide concept of "facilitating" a relationship with a user, the scope of this is much larger than what the drafters may have envisaged.[94] As AI companions do not necessarily have to be information society services, any soft toy that uses on-device emotion detection to alter its functionality, even by choosing between pre-programmed phrasing, would fall under this provision. A classic example is Paro the Seal, a fluffy white 2001 therapeutic soft toy and arguably the world's best-known care robot, which would fall within the scope of this provision. Paro would in fact not just fall within this provision, but may be prohibited by it. It intrinsically uses microphones for its functionality, arguably prohibited for children under 15 and has no mechanism for discerning who is or is not

89: *Id.* recital 30.
90: *Id.* art. 20(4)(b).
91: Unless Pokémon Go is also a social network, this technically hinges on whether Article 15(1)(b) of the Proposal, applying to online games, which imports Article 11(1), impliedly must import Article 11(2) into scope in order to make the whole regime make sense. Again, this is poor drafting.
92: *KIDS Act Proposal*, *supra* note 9, arts. 14(1)(b), 11(2).
93: *Id.* art. 3(5)(c).
94: *See KIDS Act Proposal*, *supra* note 9, art. 3(3), (5)(c) (adopting the AI Act's definitions of "AI system" and "general-purpose AI system," and defining an AI companion as "an AI system, including a general-purpose AI system," that "simulates or facilitates a social, emotional or interpersonal relationship with a user"). *Compare* AI Act, *supra* note 28, art. 3(1) (defining an "AI system"), *with id.* art. 3(66) (defining a "general-purpose AI system").

that age because it is a soft toy.[95]

The Proposal needs to be clear about what it means. The "default settings" framing is incredibly uncertain. Under what conditions can children under 15 use a service that inherently relies on geolocation, a camera, a microphone, or a recommender system?

IV. AWKWARD REALITIES OF AGE ASSESSMENT

The Proposal expects, and indeed relies upon, multiple infrastructures to prove, estimate, and attest different facts about children and adults. It relies on age assurance tools, which are designed and implemented by services and must meet certain criteria.[96] In certain situations, it relies upon age verification tools, which connect to a very specific European regime concerning identities and proof.[97] It also relies upon parent and guardian attestation tools, which will in practice intertwine with these age verification tools, and which are to be specified in a delegated act.[98] All of these have complexities and oversights that are not on the face of the Proposal and are likely to create significant issues in the future.

A. AGE ASSURANCE

As anyone familiar with the technolegal discussions of children online will know, age-gating can be powered by either age verification or age estimation.[99] The latter is sometimes called age assurance (in contrast to verification), but the Proposal uses 'age assurance' to cover both age verification and age estimation as an umbrella category.[100] Age verification can be characterized technically as the process of verifying an identity and then verifying that that identity is connected to an attestation of age that comes from a trusted source, such as a government.[101] Age estimation refers to a probabilistic inference of age from various signals that vary massively in quality and reliability.[102] Even where age estimation functions and uses the best facial recognition algorithms, for teenagers it typically brings an error margin of 3–5 years, meaning that while such systems might be able to tell a 12 year old from an adult with confidence, they will struggle to reliably distinguish between 16 year olds and 18 year olds.[103]

95: *Id.* arts. 14(1)(b), 11(1)(b). *See generally* Michaela Pfadenhauer & Christoph Dukat, *Robot Caregiver or Robot-Supported Caregiving?*, 7 Int. J. Soc. Robot. 393 (2015) (discussing Paro's functionality).

96: *KIDS Act Proposal*, *supra* note 9, ch. V.

97: *See generally* Martin Sas & Jan Tobias Mühlberg, *Trustworthy Age Assurance? A Risk-Based Evaluation of Available and Upcoming Age Assurance Technologies from a Fundamental Rights Perspective*, Greens/EFA Eur. Parliament (Feb. 2024), https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf [https://perma.cc/XA72-TQR8] (appraising the qualities and features of the envisaged technical instruments in the context of European law).

98: *KIDS Act Proposal*, *supra* note 9, art. 26; these are analyzed *infra* Part V.A.

99: *Id.*, recital 53.

100: *Id.*, art. 3(5)(i).

101: *See* Nat'l Inst. of Standards & Tech., *Digital Identity Guidelines*, NIST SP 800-63-4, § 4 (2025), https://pages.nist.gov/800-63-4/sp800-63/model (separating identity proofing from authentication, which requires "possession and control of … authenticators that are bound to the subscriber's identity").

102: Zahra Stardust et al., *Mandatory Age Verification for Pornography Access: Why It Can't and Won't 'Save the Children'*, Big Data & Soc'y, Apr.–June 2024, at 1, 3–4 (describing age estimation tools and reporting success rates of 70–87% across studies, so that roughly one in five subjects is placed in the wrong age group).

103: Wouter Lueks et al., Assessing Age Assurance Technologies: Effectiveness, Side-Effects, and Acceptance (Mar. 26, 2026) 18, http://arxiv.org/abs/2603.25695.

The broad structure of the KIDS Act Proposal is that age *verification* is a requirement for social networks' and video platforms' delayed account creation provisions.[104] Such age verification technologies must be certified by an EU certification scheme also seeded by this Proposal.[105] For the design-based obligations, insofar as those also require or imply that the age of the user is known or could be guessed at, these can function through any age assurance technologies, but only if they provide a "high level of accuracy, reliability, security, robustness, non-intrusiveness, privacy and data protection, and non-discrimination," and do not "enable the identification of the recipient nor locate, track, target, advertise to or profile recipients for any purpose," as well as other criteria considered later.[106]

B. AGE ASSURANCE... WITHOUT DATA?

The DSA, in its provisions on the protection of minors, states that "[c]ompliance [...] shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor."[107] The Proposal "specifies and complements" but does not amend or repeal this provision, allegedly to "operationalise the obligation to put in place a high level of privacy, safety and security of minors."[108] Yet it is quite clear that while the DSA may not oblige providers to process additional personal data in order to assess whether the recipient is a minor, the Proposal does and attempts a U-turn on a piece of text that was seen as a blocker to regulatory action. "Additional" in the DSA clearly, in light of the recitals, means additional to what the platform already processes;[109] however, while the Proposal obliges providers to "maintain, acquire and process" no more than the personal data sufficient for the purpose of age assurance, this is still more than they would have processed beyond their existing business models.[110] The DSA could fundamentally not support much in the way of age assurance or verification with that restriction remaining in place. Yet the Proposal can be easily criticized for not addressing this head-on. Amending would be more honest and elegant than pretending nothing has changed.

The biggest tensions between obligations and data-processing limitations, however, come from within the Proposal itself. For example, the Proposal goes to great lengths to mandate privacy-related conditions for age verification solutions. It mandates that "[a]ge assurance solutions shall not enable the identification of the recipient nor locate, track, target, advertise to or profile recipients for any purpose."[111] It also states, in somewhat questionable grammar, that "[a]ny age assurance measure shall be zero knowledge proof."[112]

All this falls apart when the rest of the Proposal, or indeed the field of privacy engineering, is considered. A zero-knowledge proof is a cryptographic protocol that demonstrates a statement

104: *KIDS Act Proposal*, *supra* note 9, art. 29(2).
105: *Id.*
106: *Id.*, arts. 27, 28(1).
107: Digital Services Act, *supra* note 6, art. 28(3).
108: *KIDS Act Proposal*, *supra* note 9, art. 1, recital 5-6.
109: Digital Services Act, *supra* note 6, art. 28(3) & recital 71 (explaining that, consistent with the GDPR's data minimisation principle, the prohibition on profiling-based advertising to minors "should not lead the provider of the online platform to maintain, acquire or process more personal data than it already has in order to assess if the recipient of the service is a minor," and "should not incentivize providers of online platforms to collect the age of the recipient of the service prior to their use").
110: *Id.* recital 51.
111: *Id.* art. 28(1).
112: *Id.* art. 28(3).

without revealing the process of proving that statement.[113] Physical identity cards can be set up, for example, to prove that your age is greater than the age required by the person you are trying to prove the fact to, without revealing your date of birth. Age verification technologies, if engineered correctly, can indeed be designed to present zero-knowledge proofs to the entity seeking an attestation. Not all are, but it is possible.

However, zero-knowledge proofs as a technology are meaningless when applied to age *assurance* technologies, as the Proposal does. These technologies try to estimate ages based on signals such as facial imagery, voice and video, document scans, or the patterns of typing or service use.[114] Such mechanisms are not mentioned in the Proposal, which talks generically about methods that can establish age with a "high degree of confidence," but these methods are what the term age assurance refers to in both European and international policy circles.[115] Furthermore, the explicit reference encouraging using "reliable information such as through previously legitimately acquired credit card details" to undertake it on existing users simply cannot be zero-knowledge by nature, as the provider already holds and has knowledge of the information.[116]

If the zero-knowledge proof requirement is to be taken literally, age assurance based on face, for example, is unlawful as a compliance approach under the Proposal. This seems somewhat unlikely but makes it extremely hard to assess what the Proposal is, well, proposing.

Further contradictions emerge. Despite how age assurance solutions "shall not enable the identification of the recipient nor locate, track, target, advertise to or profile recipients for any purpose," providers should, somehow, "limit the creation, by minors, of secondary accounts aimed at circumventing safety by design measures." [117] To identify someone by their digital fingerprint when they are logged out of their account inherently requires identifying and tracking them for a purpose. The Proposal sets up many difficult, arguably impossible, tensions and asks even the smallest social networks or video platforms, by virtue of the Proposal's wide scope, to solve them.[118]

113: For the curious and for the pedants who want something more complete, a zero-knowledge proof ("ZKP") is a cryptographic protocol by which one party (the "prover") convinces another (the "verifier") that a statement about secret information is true, without revealing anything about that information beyond the fact that the statement is true. *See* Kenneth A. Bamberger et al., *Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs*, 37 Berkeley Tech. L.J. 1, 28–31 (2022). A valid ZKP has three properties: *completeness* (a true statement will be accepted), *soundness* (a false statement will be rejected, even if the prover cheats), and *zero-knowledge* (the verifier learns nothing it could not have generated on its own). *Id.* at 29. The idea is really quite headache-inducing and notoriously hard to explain, but may be illustrated by someone who claims he can instantly count the needles on a pine tree: a skeptic secretly plucks a handful and asks the person with the claimed power how many she is now holding. If he answers correctly, she is convinced (as he knew the difference between the pine tree then-and-now), but she doesn't learn anything new (e.g. about the actual number of needles on the tree), and she already knew the number she had snagged in her hand. *Id.* at 30–31. In the context of age verification, a ZKP could let a user prove that some government-issued credential certifies she is over eighteen without disclosing her name, date of birth, etc. *Cf. id.* at 28–29 (describing a driver who proves her license is valid without revealing her exact age).

114: *See* Sas & Mühlberg, *supra* note 97, at 50–57. This is assuming that the provider is the one undertaking such analysis; if such analysis was undertaken by a user on their own device, there may be some role for a technology such as a zero-knowledge proof. This is clearly not what the Regulation is contemplating.

115: *KIDS Act Proposal*, *supra* note 9, art. 32(2)–(3), recital 61.

116: *Id.* recital 61.

117: *Id.* art. 28(1).

118: *Id.* recital 18. This, however, is an obligation in a recital that is missing from the relevant operative article (presumably Article 4), a sign of poor drafting.

C. WHEN IT GOES WRONG

Many of these age assurance systems are also going to fail or misclassify people. The Proposal requires an "effective internal complaint-handling mechanism" when people are misclassified, but only that.[119] Other EU instruments that reflect disabled accounts, such as the DSA or the Directive on Platform Work, provide for much more detailed procedural safeguards, such as the obligation to review the decision in a non-automated manner.[120] By contrast, the only conditions the Proposal places on such processes are that they should be "effective" and "free of charge."[121] Those excluded from a service under the Proposal have no recourse to a regulator to challenge an individual decision (rather than general non-compliance),[122] nor access to an out-of-court dispute settlement body. This is questionable under European law; such decisions would likely be classified as significant, solely-automated decisions taken on the grounds of Union law.[123] This requires that same law to "[lay] down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."[124] A complaint-handling mechanism is a procedural obligation. It is not a substantive safeguard.

D. OR JUST TIMES OUT

Such recourse will be needed at scale after a six-month period from the Proposal entering application, whereby any account on any covered provider "in relation to whom the age cannot be established" must be disabled.[125] Or it may not. It seems quite clear that this is a fantasy that simply will not happen.

In order for such a mass disabling of accounts to occur after six months, a significant number of unspecified parts must exist. The Commission must have published implementing acts specifying the EU Age Verification Scheme and delegated acts on "alternative age assurance," guardian tools, and ideally, parental responsibility signals if it is not just going to be blind self-attestation (discussed below in Part V.A.).[126] National public authorities must have certified solutions for use for age-gating, which can only happen after the scheme has been published. Things need to be built, too. Member States should have made available one functioning, approved, entirely free age verification solution for citizens and residents.[127] Member States also, for the Proposal to function meaningfully, need to have created an entirely new infrastructure for digital attestation of parental responsibility, with all the many complications it brings. No deadline has been attached to the provision of either service. This is quite clearly not going to happen within six months, and for the Commission to even claim that it might seem disingenuous. The DSA had over a year for its

119: *Id.*, art. 29(5).
120: Digital Services Act, *supra* note 6, art. 20(6); Directive 2024/2831 of the European Parliament and of the Council of 23 October 2024 on Improving Working Conditions in Platform Work, arts. 10–11, 2024 O.J. (L 2831) 1, 53 (EU).
121: *KIDS Act Proposal*, *supra* note 9, art. 29(5).
122: *See KIDS Act Proposal*, *supra* note 9, art. 21.
123: *See* GDPR, *supra* note 32, art. 22(1), (2)(b).
124: *Id.* art. 22(2)(b).
125: *KIDS Act Proposal*, *supra* note 9, art. 6(4).
126: *Id.* arts. 20(7), 26(5), 30(2), (3)(a).
127: *Id.* art. 31(5).

main provisions; the EU AI Act, following the Omnibus, is set for three to four years.[128]

V. TOOLED-UP GUARDIANS

Much of the Proposal hinges on the so-called "tools for guardians" that are required by the majority of in-scope services.[129] These, too, face significant practical and interpretive problems, both in identifying guardians in the first place, and implementing tools in the messy realities of childhoods we see across Europe.

A. WHO ARE THE GUARDIANS? PROBLEMS OF PARENTAL ATTESTATION

Parent and guardian attestation tools are an important part of the Proposal. The Commission intends to specify how these should work in a delegated act.[130] They may, however, find the task a more difficult one than perhaps they anticipate.

1. Defining the Guardians

The definition of guardian in the KIDS Act Proposal is "any person holding parental responsibility over a minor pursuant to applicable national law."[131] The KIDS Act Proposal anchors this definition to the definition of "parental responsibility" in the Brussels IIb Regulation, which "means all rights and duties relating to the person or the property of a child which are given to a natural or legal person by a decision, by operation of law or by an agreement having legal effect, including rights of custody and rights of access."[132]

This chain of definitions creates issues and ambiguities. First, in many cases where children live with kinship carers, there will be no formal order or record stating that this is the case to digitize. Depending on the degree to which the whole KIDS Act framework is enforced, this either excludes children from digital services or excludes these carers from the guardian tools. Second, a similar situation arises with foster parenthood, where official parental responsibility often remains with an institution or the parent, rather than the day-to-day carer, and this varies across Europe.[133] The KIDS Act Proposal does not seem to fit the idea that an institution, rather than an individual, might be the user of these guardian tools. In an ideal world, the attestation infrastructure would capture the individual who could, in practice, best help the minor with their digital life by exercising rights that arise from some position of guardianship or responsibility.

128: *Compare KIDS Act Proposal*, *supra* note 9, art. 43 (applying from six months after entry into force, with Articles 33 and 35 applying from twelve months), *with* DSA, *supra* note 6, art. 93 (entering into force on the twentieth day after publication on October 27, 2022 and applying in full from February 17, 2024), *and* AI Act, *supra* note 28, art. 113 (applying obligations for high-risk AI systems listed in Annex III from December 2, 2027, and for those covered by Annex I from August 2, 2028, against entry into force on August 1, 2024).

129: *See, e.g., id.* arts. 20 (outlining "tools for guardians" framework); 20(4) (directing providers to integrate "tools for guardians" with other mechanisms in the Proposal; 3(5)(p) (defining "tools for guardians").

130: *KIDS Act Proposal*, *supra* note 9, art. 26.

131: *Id.* art. 3(5)(b).

132: *Id.* recital 15; Council Regulation 2019/1111 of 25 June 2019 on Jurisdiction, the Recognition and Enforcement of Decisions in Matrimonial Matters and the Matters of Parental Responsibility, and on International Child Abduction (Recast), art. 2(2)(7), 2019 O.J. (L 178) 1 (EU).

133: Josep Ferrer-Riba, *Parental Responsibility in a European Perspective*, *in* 3 European Family Law: Family Law in a European Perspective 284, 296–97 (Jens M. Scherpe ed., 2016), https://doi.org/10.4337/9781785363054.

The diversity of individuals who that might be is extremely far from being digitizable or even provable with conventional and verifiable documents. The Proposal does oblige Member States to create a parental attestation system that is accessible to "persons in vulnerable situations such as refugee and displaced families."[134] This is more of an aspiration than a roadmap.

This can get complex fast. In many European countries, including Austria, France, Italy, Portugal, and Spain, joint exercise of parental authority is generally maintained even where there is a protection order or where a parent has been convicted of violence.[135] The Proposal neither obliges service providers to keep the provision up to date nor provides a mechanism for the child or another actor to trigger a reassessment of parental responsibility. Legal orders may restrict the exercise of parental responsibility without removing it, but these orders are unlikely to address the online supervision of children as a specific item. Even if the data were available, this leaves uncertainty as to what the service provider should do with this information. Children can be in vulnerable situations here unless this is taken care of, being surveilled by people who should not have access to their accounts or digital lives.

2. Look Mom, No Data

Many Member States simply do not have reliable digital data sources even for conventional guardianship situations, let alone complex ones. Several Member States lack even basic infrastructure for simple parental attestation. For example, in Ireland, one way for an unmarried father to obtain joint guardianship with the mother is through a statutory declaration signed by both parents.[136] When this is used, this witnessed form is the *only* proof of such guardianship existing: there is no central registry for these statutory declarations.[137] Elsewhere in Europe, the administrative structure throws a spanner in the works. German population registers and French civil status records are heavily decentralized to thousands of authorities.[138] Such records are not considered authoritative on custody orders, and the processes that are authoritative are complex and time-consuming.[139] The Proposal states that Member States must provide "appropriate alternative procedures where parental responsibility cannot be demonstrated through standard

134: *KIDS Act Proposal*, *supra* note 9, art. 31(2). It does not deal with the arguably more conventional parental responsibility issues that family law also has to cope with day to day.

135: Council of Eur., Grp. of Experts on Action Against Violence Against Women & Domestic Violence [GREVIO], *Thematic Perspectives on the Implementation of the Istanbul Convention*, at 57–58 (Mar. 2025), https://rm.coe.int/thematic-perspectives-on-the-implementation-of-the-istanbul-convention/1680b4a2e3 [https://perma.cc/MVU9-7BYT].

136: *Guardianship Information*, Treoir (Sept. 10, 2026), https://treoir.ie/information/guardianship-information/ [https://perma.cc/2KVJ-8TW7].

137: *Id*.

138: *See generally* Birgit Feldtmann et al., *Facilitating Life Events: Part II: Synthesis Report* 12 (2008) (study for the European Commission, No. JLS/2006/C4/004), http://www.freyvial.de/Publications/Civil_Status_in_Europe_Synthesisreport.pdf (classifying Germany and France among "event-based" systems in which civil status registers are kept locally where each event occurred).

139: On Germany, *see generally* Bundesnotarkammer [Federal Chamber of Notaries], *Stellungnahme zum Entwurf eines Kindschaftsrechtsmodernisierungsgesetzes (KiMoG)* 3–5 (July 10, 2026), https://www.bnotk.de/fileadmin/user_upload_bnotk/Stellungnahmen/2026/BNotK_STN_2026_KiMoG.pdf (explaining that unmarried parents prove custody *only* by producing their notarized custody declarations or, for sole maternal custody, a written statement from the custody register, which is available to mothers alone); on France, *see* Réponse ministérielle n° 117359, J.O. Assemblée Nationale, Feb. 28, 2012, p. 1881 (Fr.) https://www.assemblee-nationale.fr/dyn/13/questions/QANR5L13QE117359 (explaining that parental authority for minors' passports is verified from a birth extract and the statutory presumption of joint authority, and that the *livret de famille* is no longer accepted specifically because its entries are not systematically updated).

civil status documentation."[140] For many Member States, this will be an enormous, potentially expensive, and largely manual undertaking.

3. The Politics of Pan-European Parenthood

Even if verified documents were provided, the same verification would run into cross-jurisdictional problems. Migration and free movement create an enormous and largely unstated problem in this Proposal. Member States are only obliged to provide parental responsibility infrastructure in relation to those "residing in their territory."[141] The parentage of same-sex couples, or parental responsibility arising from surrogacy, may not be recognized in the same way in all Member States. The Commission itself estimates that two million children may face difficulties obtaining recognition of their parentage for all purposes in another Member State. Its proposed solution, the European Certificate of Parenthood, has, at the time of writing, never escaped the Council.[142] Given the controversies over the proposed Certificate of Parenthood, how will the Member States react to having unanimity around issues of parenthood information and signals taken away from them and replaced with market harmonization, only requiring a qualified majority of Member States to agree to it for it to proceed through the legislative process?[143] Politically, the Proposal could be torpedoed on this basis, and without parental attestation infrastructure, the Proposal does not meaningfully function.

In practice, this means that the infrastructure being required of Member States in the Proposal cannot simply be conjured into existence as a matter of technocracy. It requires enormous investment, political will, and mutual recognition that has previously been a serious stumbling block.

4. Expect Self-Declaration

Ultimately, the Commission will be unable to solve this sociotechnical and political challenge through a delegated act. Providers will have to accept self-declaration, which remains an option at least until the Commission passes a delegated act outlining how the parental recognition infrastructures could or should work.[144] Yet the service provider, when accepting such declarations, has to "make reasonable efforts to verify that the adult making the self-declaration is exercising parental responsibility." The verification must also be carried out "in a privacy-preserving manner" and

140: *KIDS Act Proposal*, *supra* note 9, art. 31(3).

141: *Id.* art. 31(2).

142: Proposal for a Council Regulation on Jurisdiction, Applicable Law, Recognition of Decisions and Acceptance of Authentic Instruments in Matters of Parenthood and on the Creation of a European Certificate of Parenthood, COM (2022) 695 final (Dec. 7, 2022), https://data.consilium.europa.eu/doc/document/ST-15837-2022-INIT/en/pdf [https://perma.cc/U3XT-EY3A] [hereinafter ECP Proposal]. *See generally* Stefan Rakic & Jiyu Choi, *Parent in One Member State, Parent in All Member States: The Good, the Bad and the Ugly*, 8 Eur. Pap. - J. Law Integr. 1555 (2023), https://doi.org/10.15166/2499-8249/730 (discussing the political obstacles). Note that in the Commission's own Impact Assessment as compared to the preamble of its proposal, the number of "mobile parents" and their children affected is given as 103,000. *See* European Commission, *Impact Assessment Report Accompanying the Document Proposal for a Council Regulation on Jurisdiction, Applicable Law, Recognition of Decisions and Acceptance of Authentic Instruments in Matters of Parenthood and on the Creation of a European Certificate of Parenthood*, SWD (2022) 391 final (Dec. 7, 2022) 21, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022SC0391 [https://perma.cc/M5YT-QABF].

143: Consolidated Version of the Treaty on the Functioning of the European Union arts. 81(3), 114(1), June 7, 2016, 2016 O.J. (C 202) 47.

144: *KIDS Act Proposal*, *supra* note 9, art. 26(1)(c), 26(5).

"shall not lead to additional processing of personal data that could enable the provider to determine the location of the adult or minor concerned or to track, target or profile the adult or minor."[145] It is very likely that in a huge number of cases, the only method to verify parental responsibility would be through the provision of a document, which will be in the language of a Member State, and contain hugely revealing information about the child. This is a non-starter, both in terms of compliance—are tiny social networks going to robustly verify parental documentation in Maltese?—and in terms of meeting the privacy obligations set out in the Proposal.

As a result, while Member States are tasked with building an impossible infrastructure and resolving private international law discussions about who is considered to have parental responsibilities across Europe, anyone, stranger or not, will be able to attest to being the guardian for any child. This is almost the case even if a parental attestation system is built. This is because children often lack identification documents of their own, for multiple reasons. Some Member States (such as Ireland) lack national ID cards entirely.[146] Other Member States (such as Germany) do issue them, but disable by law the functionality that allows them to be used for online identity verification.[147] It will often therefore not be possible to verify the user is a specific child. Even where a digital attestation of parental responsibility is possible due to the data being available, services will often end up only verifying that a specific adult has parental responsibility over *some* child. While the Proposal requires providers to make reasonable efforts to verify parental responsibility,[148] there appears from the above analysis, at least in some Member States, to be no such possible efforts which are reasonable for a regulated service to rely on. Services may have to verify a proposed parent or guardian is an adult—the Proposal is strangely silent on whether a parent has to use an age verification process to verify their own age or whether assurance will do for that too—but they will seemingly not have to do much more than that.

B. THE LONG TAIL OF KIDS AND FAMILIES

Children's lives are not idyllic. Some are very difficult, turbulent, and saddening. The entire Proposal focuses heavily on the vulnerabilities that emerge from being a child, and dedicates effectively no space to how these measures will work for and impact disproportionately vulnerable categories of children. It is not difficult to think of a huge number of situations to which this Proposal is ill-prepared to respond to.

The structure of the social network and video platform derogations for minors aged 13 to 15 places the guardian in a significant position of power over the child. For example, tools enable guardians to disapprove contacts and set a maximum time per day up to one hour (presumably including zero). The guardians must be able to report content the child encounters on their behalf, indicating they have at least some visibility over what the child is seeing. The recitals anticipate that guardians will have access to monitoring tools, such as flagging "repeated searches"

145: *Id.* art. 26(3)–(4).

146: Editorial, *The Irish Times View on the Public Services Card: Overstepping the Mark*, Irish Times (Aug. 2019), https://www.irishtimes.com/opinion/editorial/the-irish-times-view-on-the-public-services-card-overstepping-the-mark-1.3991246 (noting that Ireland "is one of three EU states that does not issue national identity cards").

147: Gesetz über Personalausweise und den elektronischen Identitätsnachweis [Personalausweisgesetz] [PAuswG] [Identity Card Act], June 18, 2009, BGBl. I at 1346, §§ 10(2)–(3), 18(1) (Ger.) (requiring the card manufacturer to switch off the electronic identity function where the applicant is under 16, allowing it to be switched on only once the holder is 16).

148: *KIDS Act Proposal*, *supra* note 9, art 26(3).

the child makes about harmful topics.[149] It is welcome that the law proposes the child should always be made aware of any tool's use in real time. However, no exemptions here are present for services designed to protect children or enable them to report abuse by their guardians. Exact measurements and methodologies differ, but parents typically represent the highest proportion of abusers—much more than strangers—in relation to child mistreatment and neglect other than sexual abuse.[150] It should not be the case that parents have the ability to block, or even monitor, their child's attempts to seek help when they may be in an abusive situation.

Further, often related issues emerge as guardian responsibilities can change throughout a child's life, especially in turbulent or abusive situations. Children go in and out of care, they can lose a parent or be orphaned, and they can be taken away from guardians while legal proceedings determine guardianship. Parents may become estranged or divorced, and there will be situations where both want to oversee a child's digital life, or where one has authority and uses it in a way the other disagrees with, for example to entirely block a child's accounts by reducing daily time to zero, or to deny them contact with one side of the family. The Proposal states that providers should actively limit children from making secondary accounts, limiting the child's ability to mitigate this tension.[151] The Proposal does not even allude to how change of guardianship works, and the significant difficulties in migrating a child's account (and their connections, digital life, and history) from one guardian to another, or how providers should reconcile competing demands from individuals claiming to be a child's guardian or disputing the self-declaration of the other. This is a serious omission. To ignore this is to ignore, and even exacerbate, the struggles of an enormous number of children throughout Europe.

C. ONE API PER CHILD

The Proposal states that:

> Providers of very large online platforms designated in accordance with Article 33 of Regulation (EU) 2022/2065 shall ensure that the tools for guardians referred to in paragraph 1 are interoperable with tools for guardians provided by third parties, in accordance with the conditions set out in Article 6 of Regulation (EU) 2022/1925, where relevant.[152]

This paragraph needs some unpacking. There is a strange overlap between two of the main threshold-based digital laws passed by the EU in recent years. The start of the provision refers to the "very large online platforms" (VLOPs) of the DSA, designed to regulate the design and moderation of large online platforms. Yet the end of the provision refers to Article 6 of the DMA, designed to temper the economic power of large firms—an obligation that applies specifically to a handful of designated "gatekeepers."[153]

It is unclear whether this is intended to mean that only entities that are *both* VLOPs and gatekeepers would be addressed under this part of the Proposal (a cross-over reading), or whether

149: *Id.* recital 43.

150: Admin. for Child. & Fams., U.S. Dep't of Health & Hum. Servs., Child Maltreatment 2024, at xii (Jan. 16, 2026), https://acf.gov/sites/default/files/documents/cb/cm2024.pdf [https://perma.cc/EW7F-AQPW] ; Off. for Nat'l Stat., Abuse During Childhood in England and Wales: March 2024, at 10 (Nov. 5, 2025), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/abuseduringchildhoodinenglandandwales/march2024 [https://perma.cc/VN2W-MHAQ].

151: *KIDS Act Proposal*, *supra* note 9, recital 18.

152: *Id.* art. 20(5).

153: Digital Markets Act, *supra* note 11, arts. 3, 6; Digital Services Act, *supra* note 6, art. 33.

it would apply to all entities that qualify as VLOPs (an all-VLOPs reading). The cross-over reading is supported by how this provision does not even mention the relevant paragraph of Article 6 to import it. It surely cannot be the case that all provisions are importexd wholesale; Article 6 contains a whole range of provisions. The reference may just be a reminder that Article 6 extends to the guardian tooling in cases where it usually applies. Yet if we adopt such a cross-over reading and look for firms that are in the intersection who are both VLOPs and gatekeepers, these are only ByteDance's TikTok, Meta's Facebook and Instagram, Alphabet's YouTube, and Microsoft's LinkedIn. The interoperability provisions in Article 6, namely Article 6(7), are scoped only to apply to operating systems and virtual assistants, not social networks or similar services. Article 6(7) is therefore incapable of applying to parental tools, except perhaps regarding AI systems, insofar as they are virtual assistants. If the Commission intended Article 6(7) to apply *mutatis mutandis*, it should have said so. Better yet, it should write out what it actually means as an obligation that makes cogent sense.

Perhaps instead we should assume the all-VLOPs reading, disapplying the DMA scope and applying Article 6, or even generously narrowing it to Article 6(7), *mutatis mutandis*. This is supported by the phrasing of the relevant recital.[154] Yet this too brings enormous confusion. Which parts of Article 6 apply to VLOPs? Who enforces them, and with what powers, given that the DMA powers extend only to enforcement against designated gatekeepers?[155]

In any case, connecting the guardian tools obligation to the DMA is a lazy and conceptually confusing way to achieve policy aims. The relevant DMA interoperability provision is intended to limit gatekeepers' ability to create privileged ecosystems, for example, by pushing customers to buy a wearable device because it is the only one that works with their phones.[156] Placing a regulatory obligation on a firm to undertake a certain practice does not necessitate that this regulatory obligation should therefore become a market. The obligation is designed to make things easier for guardians to manage their child's online life across multiple services in one place. This is a clear public good that does not need to be shoehorned into the DMA's attempt, *ex ante*, to prevent market dominance. Interoperability has public benefits because of the agency it grants individuals, not just because of the markets it might create.

Moreover, lacking from this provision are obligations relating to security and privacy connected to such APIs. Do these firms have to offer API integration to any firm, regardless of its trustworthiness? Or can they apply security criteria, given that this is very sensitive data concerning children? Recent interoperability provisions concerning content data have allowed such security considerations to factor into the process for a reason.[157] Yet in the Proposal, no clear obligations to ensure privacy and security are applied to these third parties.

D. STALKERWARE PARADISE

Care is needed around these guardian tools, because the existing market for "parental control apps" is effectively the presentable face of stalkerware. Intimate partner abusers are documented to abuse their victims through their children, including explicitly by stalking and surveilling the victim via

154: *See KIDS Act Proposal*, *supra* note 9, recital 43 ("For very large online platforms within the meaning of Article 33(1) of Regulation (EU) 2022/2065, interoperability with third-party guardian tools should further enhance usability and effectiveness, in accordance with conditions set out by Article 6 of Regulation (EU) 2022/1925.").

155: *See* Digital Markets Act, *supra* note 11, art. 29(1).

156: *See id.* recital 55.

157: *See id.* art. 7(9).

children's devices.[158] But there is another misuse vector that needs careful consideration, and one which will almost certainly emerge with the Proposal as written. These guardian control tools will be used to control the accounts of adults, rather than children.

Adults regularly use parental control apps to control the accounts of other adults. Sometimes this is for innocuous, consensual, and playful reasons—such as such apps' use as methods of tracking and control in BDSM communities.[159]

But many times, these same tools are used to enable intimate partner abuse. Researchers have noted that child monitoring apps often provide "some of the richest capabilities" for intimate partner violence.[160] Yet nowhere in the Proposal is there an obligation to protect adults whose accounts have been abusively restricted and surveilled as if they were minors. For example, such safeguards might include ensuring accounts are labeled as minors when displayed to third-party contacts, or permitting third-party connections who are interacting with someone whose account has been restricted as a minor to be able to file a report if this is incorrect to lead the platform to take action. There is seemingly no obligation for a platform to prove with a high degree of reliability that an account belongs to a child before surveillance capabilities can be enabled. The issue with a "safe by default" world is that when such safety includes surveillance, it creates an environment where abusers can thrive, also by default.

Abuse may also occur through two separated parents monitoring the same child's account. "Using the child" is a long-understood method of coercive control. In technology-facilitated violence, studies have indicated that children's devices are used by abusers to read or monitor communications between the child and others in order to learn more about and control the victim-survivor.[161] The Proposal is silent both on this and on times when two separated parents both seek access to a child's digital life—and what happens if their wishes conflict. Conflict and the weaponization of a child are not issues that can be simply solved by technology or settings, but they both must be deeply incorporated into thinking and rulemaking.

VI. DESIGNING GOOD CONTENT IN AND BAD CONTENT OUT

Finally, we turn to the broad design obligations that concern content in the Proposal. Much has been written about the impact of design obligations on, for example, minoritized content or adolescent sexual discovery.[162] This Article is more focused on the textual issues in the law than

158: *See* Anniina Kaittila, Sonja Tihveräinen, Outi Kekkonen, Johanna Hietamaki, Suvi Nipuli, Sisko Piippo, Hanna Mielismäki, Annamari Kangas-Kalinen, Elli Hyväri, Leo Nyqvist & Marita Husso, , *Children's Involvement in Technology-Facilitated Violence (TFV) in the Context of Intimate Partner Violence (IPV): Experiences of Professionals Working with Victims of Violence in Finland*, 173 Child Abuse Neglect art. no. 107878, at 6 (2026).

159: *See, e.g.*, Alison Sinkewicz, *A Data Dominatrix Showed Us How Our Online Privacy Is Violated*, VICE (Apr. 27, 2018), https://www.vice.com/en/article/a-data-dominatrix-showed-us-how-our-online-privacy-is-violated/ [https://perma.cc/FJ48-PK63]; Magdalene Taylor, *The Kinksters Using HR Software to Let Others Control Their Private Info*, MEL Mag. (May 17, 2022), https://melmagazine.com/en-us/story/anydesk-teamviewer-blackmail-kink-cyber-domination [https://perma.cc/VZ4Q-S5YT]; Sexual Health Alliance, *Turn on: Technical Domination*, Sexual Health All. (Dec. 26, 2023), https://sexualhealthalliance.com/nymphomedia-blog/turned-on-technical-domination [https://perma.cc/HJ82-TZLE].

160: Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart, *The Spyware Used in Intimate Partner Violence*, *in* 2018 IEEE Symp. on Sec. and Priv. (SP) 441, 449 (2018), https://doi.org/10.1109/SP.2018.00061.

161: Kaittila et al., *supra* note 158, at 6.

162: *See, e.g.*, Ari Waldman, *Disorderly Content*, 97 Wash. Law Rev. 907 (2022); Stardust et al., *supra* note 102.

these broader, very important, debates and considerations.

A. WHAT IF THE KIDS WANT A FILTER BUBBLE?

Providers of recommender systems accessible to minors have to follow certain design principles the Proposal lays out. There are two specific provisions that create a tension that the Proposal does not reconcile.

First, providers must "ensure that the recommender systems give priority and primary weight to explicit user-stated preferences."[163] They must, however, do this while simultaneously "ensur[ing] that minors are not exposed to information suggested by the recommender systems that may pose a risk to their privacy, safety and security, including if encountered repeatedly."[164] The recitals indicate that this "should be understood as covering the so-called 'rabbit holes' or 'filter bubbles,' " where filter bubbles "[reduce] the minors' exposure to diverse content or information."[165] These pull in somewhat opposite directions: giving priority to specific user preferences inherently narrows the possibility of diversity here, while that primacy limits the ways in which filter bubbles might be tackled through injecting content that overrides narrow preferences. There are genuine questions about whether the Proposal does wish to bring "rabbit holes" within its scope. The desire to regulate "rabbit holes" but the inability to express it legally is clearly a tension, as while "rabbit holes" get three lengthy sentences in the recitals, they are not referenced at all in the operative articles, beyond a light emphasis that repeated encounters with harmful content would be undesirable.[166] If the operative articles are amended to reference rabbit holes, the legislator will need to reconcile these provisions in a principled way. Without clear direction, the firms will either make this significant trade-off themselves, or worse, use the tension to justify paralysis and non-compliance.

B. IT'S NOT GENERAL MONITORING, IT'S DETECTION BY DESIGN

The Proposal's recitals claim that "[n]othing in this [Proposal] should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers of intermediary services to take proactive measures in relation to illegal content."[167] This refers to the long-held prohibition on obliging internet intermediaries to examine each piece of content they host with the aim of ensuring they gain specific knowledge and awareness of illegality, and by doing so, lose their intermediary liability shielding.[168] In contrast to the regime in the United States,[169] intermediary liability shielding in Europe is lost if a hosting service is made or becomes aware of specific illegal content and does not swiftly disable access to it. However, if a Member State could take action that obliged a hosting service to actively look through and assess all its content for illegality, this shielding would lose practical effect for that service. The prohibition on general monitoring is designed to limit that issue.

163: *KIDS Act Proposal*, *supra* note 9, art. 10(2)(a).
164: *Id.* art. 10(2)(d).
165: *Id.* recital 28.
166: *Id.* art. 10(2)(d).
167: *Id.* recital 7.
168: Digital Services Act, *supra* note 6, art. 8; *see generally* Martin Husovec, *Prohibition of General Monitoring Obligations*, *in* Principles of the Digital Services Act (2024) (discussing the history and trajectory of this prohibition).
169: *See* 47 U.S.C. § 230.

The claim that nothing in the Proposal imposes a general monitoring obligation does not seem tenable. Consider the aforementioned requirement to "ensure that minors are not exposed" to certain categories of information that are only able to be identified analytically.[170] That requirement applies to all recommended content on a service, piece-by-piece, with an obligation of outcome. This is the specific, extreme mechanism that has previously been identified as general monitoring in European law.[171] Unlike in *Poland v Parliament*, where a related obligation, a so-called upload filter on certain copyrighted content, was upheld by the European Court of Justice, the Proposal here contains no safeguards specific to that obligation.[172] This means a service provider has to independently assess content against the risks to privacy, safety and security, rather than being given, for example, a hash of a certain piece of multimedia that they could block without assessment. If a legal obligation such as the one in the Proposal is accepted as not amounting to general monitoring, the implication is that the general monitoring prohibition in EU law does not prohibit monitoring when framed as functionally–equivalent detection by design, even if it involves independent assessment of content.

There is a recently established legal avenue out of this, but following it is extreme, and apparently not something the Commission wishes to codify or acknowledge in a statute. It is possible that the general monitoring prohibition referred to does not apply at all to a firm that operates a recommender system, as it is not to be considered a "hosting service" in the law. Two 2026 judgments of the European Court of Justice indicate that if a service goes beyond "mere categorisation and indexation" for increasing accessibility, and instead "determines, in the interest of the operator or its service, under what conditions, how and in which order of priority that information is or is not broadcast," it will lose its claim that it has no control over the content it intermediates, and therefore lose the neutral status that is a prerequisite to it receiving any shielding.[173] Given that the main area of the Proposal that implies general monitoring is inside the recommender system obligations, all providers to whom this article applies may lose their shielding. This is likely to remain an active area of legal contention.

VII. CONCLUSION: REVISE AND RESUBMIT

This Article is not about whether an EU social media ban is a good or bad idea for children, or whether there should or should not be an EU KIDS Act. It is fundamentally about under what conditions a proposed Act is fit to be put before a legislative process. This Proposal is not ready for that. The thicket of definitions in the Proposal leads to unintuitive consequences and enormous uncertainties as to the scope of the law. Recitals regularly contradict the articles, elaborate on aspects that needed to be put on the face of the Proposal, and completely omit the more nuanced aspects of the Proposal's scope—perhaps out of ignorance, perhaps because there was a hope that no one would notice. Exemptions for the long tail of services that do not pose a risk are missing, and the design obligations interact with the scope to prohibit a lot of services that seem to pose no risk, and may even be of clear benefit to some children, like book recommendations or

170: *KIDS Act Proposal*, *supra* note 9, art. 10(2)(d).

171: Case C-70/10, Scarlet Extended v. SABAM, ECLI:EU:C:2011:771, ¶¶ 35–36, 40 (Nov. 24, 2011); Case C-360/10, SABAM v. Netlog, ECLI:EU:C:2012:85, ¶¶ 25, 33–34, 38 (Feb. 16, 2012).

172: Case C-401/19, Poland v. Parliament & Council, ECLI:EU:C:2022:297 (Apr. 26, 2022).

173: Joined Cases C-188/24 and C-190/24, WebGroup Czech Republic & Others *v. Ministre de la Cultura*, ECLI:EU:C:2026:492, ¶ 112 (June 16, 2026); Case C-421/24, AGCOM v. Google, ECLI:EU:C:2026:592, ¶ 38 (July 16, 2026).

exercise trackers. The age assurance obligation to "be zero knowledge proof" is so meaningless and disconnected from engineering reality that it is insulting, and indicates that privacy engineers were not consulted during the drafting process.[174] The lack of consideration for abusive households or separated families seems to be an enormous omission, as does the lack of consideration for how "minor" accounts may be used to instead surveil adults. The parental attestation infrastructure that is envisaged is a fantasy, and one that may prove to be a political time bomb. Without a way to work out who has parental responsibility over a child, however, the whole Proposal makes little sense. The timeline is simply unrealistic and will not come to pass as the law anticipates.

There are some areas of the Proposal that can be directly improved, and there are some areas that require stepping back and rethinking more generally. This Article thus attempts to conclude with suggestions, but ultimately, argues that changes required are foundational.

A. SHIFT THE SCOPE

In terms of scope, there are clear changes that can be made to the Proposal. First, the material scope of the Proposal should be adjusted, either by avoiding definitions that originate in the DMA or by actually adopting the DMA approach that motivated these enormous definitions, to actively designate services within these broad criteria. The definitions were designed to capture a broad field, but this Proposal catches services that are so disconnected from debates about children online that it would pose an enormous (and pointless) burden to apply such obligations. The broad scope brings a lot of implicit consequences, which this Article has surveyed, including implied age-gating and impossible-to-meet design decisions for certain in-scope services. If the Proposal wishes to ban something, it should do so on the face of the statute, not as the messy and often surprising result of an interlocking series of tests and definitions. If the Proposal does not intend to ban something, the result of the tests should not end with the results they seemingly and often currently do.

Second, the Commission should clarify that clearly non-commercial services are exempted, rather than requiring them to claim, awkwardly, that non-commercial services are not information society services, as such non-commercial services are not normally provided for remuneration. The commodification of childhood is a key concern here, and where services are truly disconnected from commercial interests, it is not proportionate to include them within the Proposal. If it is desired to include non-commercial services within the scope of the Proposal, then the Commission should actually name non-commercial services that pose a significant risk to children, in order to justify the proportionality of this provision.

Lastly, the Commission should think carefully about AI systems in this Proposal. Is it really sensible that such systems continue to be promoted to all ages, while video-sharing platforms become so heavily restricted? Even for the limited obligations within the Proposal, chatbots with self-declared educational purposes already fall out of scope. Children do make real connections with real humans online, and for a human-centric world, we have to ensure that human connections are prioritized over connections with machines.

B. EMBRACE THE CHAOS

Childhood is messy. The Proposal is rosy-eyed. That needs to change.

174: *KIDS Act Proposal*, *supra* note 9, art. 28(3).

The parental attestation infrastructure does not address how the Proposal will work in non-traditional households, children in care, children of same-sex families, or children born through surrogacy moving across borders. It does not address what happens to accounts as families change over time. Member States should be given clear instructions on these and related issues, with clear design requirements and obligations to not leave children behind. This requires a period of real consultation with experts in this area, and connection to the European Certificate of Parenthood. Parental attestation is not an issue that DG CONNECT, the part of the Commission responsible for this Proposal, or indeed platform regulation more generally, should be leading. That is a matter for European family law and private international law. The Proposal also requires a technical reality check. Attestation of who is a parent requires a way to identify the child to whom that parent relates. Children do not typically have ID cards or identification methods more generally to show they are a specific child, or indeed a child at all. Parents can attest to *a* child, but how will the infrastructure know it is *this* child? Given how important parental attestation is to the Proposal, it needs a serious period of reworking and rethinking. This may involve reducing ambition elsewhere in the Proposal, rather than pretending that everything will go smoothly. Parental attestation should involve broad societal engagement, as there is only so much a technology law academic can say about family structure and tensions.

Because, as it stands and even in the presence of such attestation infrastructure, individuals only have to show plausible parenthood of *someone*, the Proposal needs active safeguards to prevent adults from locking down other adults' devices using the techniques designed to control the technology usage of children. These need to be explicit and on the face of the Proposal, as without them, the Commission is creating a pathway for intimate partner abuse.

C. SECURITY IS NOT THE AIM

It is not the purpose of this Article to debate the merits or structure of age assurance as a legal obligation. Here, the Article focuses on identifying tensions within the Proposal, rather than debating the policy direction as a whole. Yet many of the issues in the drafting do stem from an approach that imagines that, with the right infrastructures, a safe, privacy-friendly (even "zero-knowledge proof") world of age assurance and parental attestation can emerge—one that does not leave anyone behind.

This is unrealistic, for the reasons that this Article argues. A bit more modesty in the drafters' aims may be required to make this whole regime practicable on the ground rather than just appear to shine in theory. Other authors have, for example, argued for the merits of minimum social media age legislation that does not come with strict age assurance, relying instead on communicative theories of law to alter behavior rather than leaning on technoregulation.[175] Reorienting obligations and requirements in this direction creates new spaces for design, with a focus on in-person control by parents and guardians, rather than imagining that segmented, *ex ante* risk reduction by platforms will be effective rather than trivially circumvented.

These are just a few of the things that should be altered. There is, however, only so much that can be tweaked at the edges of such a deeply flawed document, regardless of whether one agrees with the policy objectives and approach. The Commission should withdraw this Proposal and

175: *See, e.g.*, Paddy Leerssen & Joris van Hoboken, *Bans Without Enforcement? On the Communicative Functions of "Social Media Ban" Legislation and the Alternatives to Platform-Side Age Assurance* (Oct. 7, 2026) (unpublished manuscript) (on file with the Georgetown Law Technology Review).

reissue a workable and realistic text.[176] If not, the Council and the Parliament will, if this law is to pass, have to do the serious analytic work that the Commission and its Legal Service failed to do in relation to this Proposal. The current drafting gives them a difficult starting point.

176: *See generally* Case C-409/13, Council v. Comm'n, ECLI:EU:C:2015:217, ¶ 74 (Apr. 14, 2015) (confirming the Commission's power to withdraw proposals).