

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

Michael Veale

Faculty of Laws, UCL and IViR, University of Amsterdam

October 1, 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, full of holes, enormous ambiguities, and unintended consequences. Recitals contradict articles. The use of scope borrowed 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 assurance of age 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.

CONTENTS

I.	Introduction	2
A.	Access	3
B.	Design	4
C.	Infrastructure	4
D.	Scope	5
1.	Territorial Scope	5
2.	Accessible to Minors	5
E.	Compliance and Enforcement	5
II.	Specific Services	6
A.	Online Social Networking and Video Sharing Platform Services	6
1.	These Aren't the Platforms You're Looking For	7

B.	Online Games	8
1.	Online Games Include All Offline Games?	8
2.	Social Networks in Trenchcoats	10
3.	Loot Boxes Banned in All Services Except Games	10
C.	AI Systems	11
1.	Limitless	11
D.	Software Application Stores	12
1.	Shared Devices	12
2.	What's in Store? Who Cares?	12
3.	An Accidental Book Ban?	13
III.	When a Setting Becomes a Ban	14
IV.	Awkward Realities of Age Assessment and Parental Attestation	15
A.	Age Assurance	16
B.	Attestation of Parenthood or Guardianship	16
C.	Age Assurance... Without Data?	18
D.	When It Goes Wrong	20
E.	Or Just Times Out	20
V.	Tooled-Up Guardians	21
A.	The Long Tail of Kids and Families	21
B.	One API per Child	22
C.	Stalkerware Paradise	23
VI.	Designing Good Content In and Bad Content Out	24
A.	What If the Kids Want a Filter Bubble?	24
B.	It's Not General Monitoring, It's Detection by Design	25
VII.	Conclusion	26

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 for both them and for society as a whole. This momentum only grew after a prohibition on certain social media services for children in Australia was rapidly passed in 2024.¹ In Europe, several countries have proposed bans in recent months and years, although 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.² Likely wary of the legitimacy costs of stopping these political demands, the

¹: Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth) (Austl.).

²: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, 2022 O.J. (L 265) 1 [hereinafter Digital Services Act]; see generally Jessica Galissaire et al., *Social Media Age Gating in the EU*, INTERFACE (May 19, 2026), <https://www.interface->

Commission in 2025 announced a “special panel of experts on child safety online,” with rapid meetings and a varied roster of participants, and quickly proposed a Regulation, the EU KIDS Act (referred to as the Proposal or EKA Proposal in this Article), to plug the gap.³

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

The Article first digs into the broad mechanics of this complex Proposal to outline its function. It then looks at the specific regulated services, and highlights tensions within them. The Article then turns to a series of thematically grouped, cross-cutting issues in the Proposal and analyzes them in context.

A. ACCESS

The Proposal prohibits account creation and account-based access below 15 for “online social networking services” (hereafter “social networks” for convenience), such as Instagram, and “video-sharing platform services” (hereafter “video platforms” for convenience), such as YouTube. These definitions are drawn from the Digital Markets Act (DMA), a regulation that places *ex ante*, competition-flavored obligations on the largest technological gatekeepers.⁴ The delayed account creation duties only apply to services exhibiting certain features that pose a “risk.” 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 intended to or with the reasonably foreseeable consequence of, “incentivis[ing] interactions with the service or with content or other recipients of the service.”⁵ Commercial services broadly attempt to incentivize consumers to use them.

Such services may, optionally, allow guardians to set up accounts on behalf of 13–15-year-olds. These accounts are limited to a maximum daily usage time, per service, of one hour.⁶ Where video platforms are specifically directed at children, they may allow under-13s to access a specially designed version of their service through their guardian’s account.⁷ It is noteworthy that explicit age restrictions on account creation are *not* placed on other in-scope services, such as AI companions.

eu.org/publications/social-media-age-gating-eu; 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. 4, 2000 O.J. (L 178) 1; *see also* Case C-188/24 and C-190/24, WebGroup Czech Republic and Coyote System, ECLI:EU:C:2026:492, ¶¶ (interpreting the E-Commerce Directive in this regard) (June 16, 2026).

³: *Proposal for a Regulation of the European Parliament and of the Council, EU Kids Act — ‘EU Keeping Internet Digital Spaces Accountable and Trustworthy’* (2026/0286 (COD)) (Sept. 17, 2026), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0681> [hereinafter EKA Proposal].

⁴: Regulation (EU) 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 277) 1 [hereinafter Digital Markets Act].

⁵: *EKA Proposal*, *supra* note 3, art. 6(1).

⁶: *Id.* art. 6(2)(b).

⁷: *Id.* art. 7.

B. DESIGN

The Proposal places feature-level design obligations on social networks and video platforms, regardless of whether they pose a risk that would bring them in scope of the delayed account creation duties. These features include limiting addictive design, functionality of recommender systems, default settings, discoverability, and economic transactions.⁸ The Proposal then selectively extends these provisions to the other in-scope services: AI systems (including companions and chatbots) and online games. Many of these provisions echo aspects of regimes in other jurisdictions, such as the UK's Online Safety Act and Age-Appropriate Design Code.⁹

Design obligations in the Proposal apply to any in-scope service that is “accessible to minors” (a test never defined). They directly remove some of the main functionality relied upon by current advertising-funded services — removing implicit engagement signals, cross-service data connection, and like counts.¹⁰ Because of this, they effectively force these services to age-gate their product, so that these features can continue to apply to their adult markets, or withdraw from the European market entirely. As a result — and as will be shown throughout this Article — the design obligations animate 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.¹¹ 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.¹² This is an extremely controversial and technical area. The Commission kicks it almost entirely into the future via implementing acts, and specifies very little about how it would work in the Proposal.¹³

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, in theory allowing users to verify on one app to a high standard, and have that signal carry over to other services they use.¹⁴ 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.¹⁵

8: *Id.* arts. 9–13.

9: Online Safety Act 2023, c. 50, §§ 11–13 (U.K.); Data Protection Act 2018, c. 12, § 123 (U.K.).

10: *EKA Proposal*, *supra* note 3, arts. 10(2), 11.

11: *Id.* art. 31.

12: Regulation (EU) No 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, 2014 O.J. (L 257) 73 [hereinafter Digital Services Act].

13: *EKA Proposal*, *supra* note 3, art. 30(2).

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

15: *Id.* art. 16(4).

D. SCOPE

1. Territorial Scope

The DSA tempers the territorial scope of its platform regulation through requiring a “substantial connection” to the Union.¹⁶ The EKA Proposal engages in no such tempering. The Proposal’s 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 placed on the Union market, following the scope of the EU AI Act.¹⁷ It 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. It 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.¹⁸ 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.¹⁹

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.²⁰

The recitals of an entirely disconnected law are hardly a good place to provide legal certainty around a difficult test. Where services are not aware of minors using the service, prohibit them from doing so in their terms of service, and there is no evidence that the service is directed at or predominantly used by minors, it could be argued that the Proposal does not apply. However, this test is simply not in the Proposal. As a recital alone rather than an operative article, it is barely even in the DSA. Amid this uncertainty, we have very little to go on around what “accessible to minors” means.

E. COMPLIANCE AND ENFORCEMENT

Enforcement is sought by grafting obligations onto three existing regimes — the national and European levels of the Digital Services Act and the AI Act, and the national data protection

¹⁶: Digital Services Act art. 3(e).

¹⁷: *EKA Proposal*, *supra* note 3, art. 2(2).

¹⁸: *Id.* art. 2(1).

¹⁹: Online Safety Act 2023, § 35 (U.K.).

²⁰: Digital Services Act recital 71.

authorities provided by the GDPR. 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.²¹ For the most part, proposed maximum fines and powers are grafted onto the fines in those regimes;²² 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 to any regulator, and thus the provisions would be unenforceable.

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 Regulation.” This is text drawn from the DMA, but at least in the case of data protection authorities who are required by the Charter to be independent of everyone, including the Commission, this is unlikely to be a legally valid provision.²³

II. SPECIFIC SERVICES

The EKA 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 unanticipated, effects on services that on the face of it might not appear to be in scope of the Regulation. Furthermore, the obligations placed on many of these services bring, especially in combination with the often very wide scope, further very 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.²⁴ Social networks and video platforms have staggered possibilities for minors to access them through accounts: first, and only for video platforms, as profiles within a guardian’s account before 13; then for both social networks and video platforms, with a guardian’s consent and as part of that guardian’s account, up until 15; and finally freely and independently from 15. At all ages, various safeguards and protective measures, in a “safety-by-design” approach,

²¹: EKA Proposal, *supra* note 3, art. 34.

²²: There are some exceptions; for example, the 6% potential fine for AI systems is higher than that in the AI Act. See *id.* art. 34(2); cf. Regulation (EU) 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. 99(4), O.J. (L).

²³: EKA Proposal, *supra* note 3, art. 34(7); Digital Markets Act art. 1(7); Charter of Fundamental Rights of the European Union art. 8(3), 2012 O.J. (C 326) 391.

²⁴: EKA Proposal, *supra* note 3, recital 21.

are mandated in a series of articles, which means that even for over-15s who can create their own accounts, the online experience will be different from that of adults.

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

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 EKA. The Proposal explicitly deems both as “online platforms” in all cases.²⁵

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 on an internship is using — as it can be used to message anyone in an organization, or, as is often the case with services such as Microsoft Teams, 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 — users can post reviews and comments visible to any other user, and, unlike the DSA, there is no ancillary feature escape route;
- Chess.com, used by competitive school chess clubs — it has forum and chat services, and as a core feature, connects players with strangers to play with.

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.

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 policy that makes it less compelling for children to read books. But for other services it is much harder to fall out of scope. 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

²⁵ *Id.* art. 3(2); *cf.* Digital Services Act art. 3(i), recital 13.

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.²⁶

There are, however, reasons that community-hosted platforms, such as Mastodon or other “Fediverse” social network instances, may fall out of scope. 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.”²⁷ 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.²⁸

B. ONLINE GAMES

The definition of online games is perhaps the most baffling in the entire Proposal, and brings significant regulatory consequences.

1. Online Games Include All Offline Games?

The definitional scope of “online games” includes many games that are functionally not online games. The definition includes “video games,” 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,” and “video game platforms,” 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].”²⁹

²⁶: Slack or Microsoft Teams could also run a more complex argument that the messaging part of their service should be analyzed separately as a number-independent interpersonal communications service, outside the EKA, 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 et seq. (June 3, 2026).

²⁷: Directive (EU) 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; Case C-484/14, *Tobias McFadden v. Sony Music Entertainment Germany GmbH*, ECLI:EU:C:2016:689, ¶ 40 (Sept. 15, 2016).

²⁸: Commission Decision of Apr. 25, 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. 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.

²⁹: *EKA Proposal*, *supra* note 3, art. 3(5)(e)–(g). 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.

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.³⁰ 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 offline but downloadable game software can enable the camera, microphone, geolocation, or push notifications during core school hours and sleep time without checking whether the user is over 15, which, given the game is offline, will be a challenge.³¹ 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.³²

There is uncertainty around whether it would create liability for resellers of physical games now also available online. The recital seems to suggest only games “exclusively” available physically are exempted.³³ 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. 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 have misinterpreted EU law in the recitals of the Proposal. The test cannot be whether a game is “exclusively” available offline, 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.³⁴ In EU law, recitals should not contradict the articles, especially not at the proposal stage before any political trading. They should explain, in natural language, the consequences of the test and the purpose of it. 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.³⁵ It could also be argued that a community-developed, open-source game is not an information society service, similar to a Mastodon instance,

³⁰: *Id.* recital 12.

³¹: *Id.* art. 15(1), instructing the application of art. 11(1). Article 11(1) appears inseparable from Article 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).

³²: See, e.g., <https://archive.org/details/classicpcgames>; <https://www.myabandonware.com/>. 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.”

³³: *EKA Proposal*, *supra* note 3, recital 12.

³⁴: Directive (EU) 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 art. 1(1)(b)(ii), Annex 1, point 2.

³⁵: *EKA Proposal*, *supra* note 3, art. 3(5)(f).

as argued above. These interpretations are far from straightforward to argue and apply.

The draft should be amended to separate out video games with no online features that allow interaction with other users as part of gameplay, and without 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, as all of these relate to either harmless features, important security provisions which 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 are faced with 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 design in 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 Regulation.”³⁶ It does not specify whether or not this deeming logic should be extended to social network–like games too. It also does not specify whether this deeming rule is an “also” considered, or if being considered as an online game under the EKA forecloses the EKA 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.”³⁷ Loot boxes are in-game purchases with an outcome determined by chance, not dissimilar to packets of trading cards. Their prevalence has raised concerns of similar psychological and financial harms as are 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.³⁸

³⁶: *Id.* recital 12.

³⁷: 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>.

³⁸: *EKA Proposal*, *supra* note 3, recitals 31, 40, art. 13(2).

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 AI Act. Neither is subject to an age ban — the EKA 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 do have an obligation to not permit under-13s to open an account other than through a guardian.³⁹

1. Limitless

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; this definition excludes 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.”⁴⁰ The definition is specifically 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,⁴¹ the educational exemption relating to “general conversational chatbot” lacks the “operated by” or “on behalf” 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 low educational quality.⁴²

The definition further trips up on what it means to be “limited.”⁴³ 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 what they were intended to do. Typically this can be assessed through either looking at the intent, the realized use of a system, or the potential use of a system, but the Proposal does not hint at which one of these conceptual categories it refers to.⁴⁴ Without such clarity, the test is effectively impossible to operationalize.

³⁹: *Id.* art. 14(1)(d).

⁴⁰: *Id.* art. 3(5)(d).

⁴¹: *Id.* art. 2(4)(c).

⁴²: See generally Marisa Meyer et al., *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) (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).

⁴³: *EKA Proposal*, *supra* note 3, art. 3(5)(d).

⁴⁴: Robert Gorwa & Michael Veale, *Moderating Model Marketplaces: Platform Governance Puzzles for AI Intermediaries*, 16 L. INNOVATION & TECH. 341 (2024).

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 services, which is focused on software applications as the intermediated product or service,” where software applications are “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.”⁴⁵ This creates some immediate scope questions.

1. Shared Devices

While the Commission may have been envisaging mobile phones when considering a software application ban, 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, and that when they kept diaries of usage, they often expressed surprise at just how much they shared and used shared devices.⁴⁶

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 may exist within an account on a streaming service. Users typically mediate this sharing through social etiquette rather than through technical controls or division.⁴⁷ Who exactly is the “recipient” of a downloaded app on an app store on a shared device?⁴⁸ How age assurance is supposed to exclude children, unless shared accounts are simply prohibited, is unclear. 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 and bring them within scope of the obligations, even though, one might hope, under-15s are generally not permitted by terms of service to make accounts for use while they are driving.

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. This appears to bring into scope low-risk services, such as browser add-on stores and the Amazon Alexa “skills” store, neither of which it is easy to imagine posing a harm to a child. Given the small number of app stores, a designation

⁴⁵: Digital Markets Act art. 2.

⁴⁶: Tara Matthews et al., “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 pp 5921–5932, 5930 (2016).

⁴⁷: See generally Ji Eun Song et al., “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 (2021).

⁴⁸: EKA Proposal, *supra* note 3, art. 16(4).

regime, rather than a regime scoped by definition and regulatee self-assessment alone, might be more appropriate.

Exemptions for certain app stores which do not appear to pose a risk to children may exist indirectly, but must be argued through the complex inter-instrumental scope rather than clearly written on the face of the Act, or even its recitals. Corporate software stores seem to escape because under the P2B Regulation, which defines the constituent definition of “online intermediation services,” users are not consumers, but employees.⁴⁹ 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.⁵⁰ 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 which is 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 system to be created for all books sold digitally by Amazon. 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.⁵¹ 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.⁵² Perhaps the CJEU will maintain, as it has in reference to a different regime, that “an e-book is not a computer program.”⁵³ Perhaps Amazon is not an intermediary of e-books, but a reseller, which changes the definitional flow.⁵⁴ 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.

49: Regulation (EU) 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. They may also not be “accessible to minors,” depending on, for example, who the firm employs.

50: *Id.* art. 2(2)(b)–(c). See generally F-Droid, *Submitting to F-Droid Quick Start Guide* (2026), https://f-droid.org/docs/Submitting_to_F-Droid_Quick_Start_Guide/ (describing F-Droid’s submission process).

51: See, e.g., Alison Flood, *Children’s Minister Raises Doubts over Age-Banding*, GUARDIAN (where 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) (Sept. 12, 2008), <https://www.theguardian.com/books/2008/sep/12/ed.balls.age.guidance.publishers.association>.

52: W3C, *EPUB 3 Overview* (Mar. 13, 2025), <https://www.w3.org/TR/epub-overview-33/>.

53: Case C-263/18, *Nederlands Uitgeversverbond and Groep Algemene Uitgevers v. Tom Kabinet Internet BV and Others*, ECLI:EU:C:2019:1111, ¶ 54 (Dec. 19, 2019).

54: Regulation (EU) 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).

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.⁵⁵ 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.⁵⁶

It is not clear what it means for a provider to change the default setting for over-15s with consent. A default is a setting 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 of under-15s. In order to enable these settings, minors must not be guided by the platform to do so, such as through notifications or promises of better functionality.⁵⁷ They certainly should not be on already, 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. 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.

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.”⁵⁸ What does this mean? Default settings might be read literally, as the default value of a setting, 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. If they refer to actual defaults, 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 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 “Default settings referred to in paragraph 1 point (a), where enabled by minors, shall be turned off after their session on the service ends.”⁵⁹ 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 it as “the above settings may only be changed by the provider where the minor is above the age of 15 and has consented.” It would mean that all references to minors changing settings were to minors for whom such setting changes were permitted, such as the over-15s. The recitals provide some support for this, giving an example of how to have a “public [account]” or “host livestream (sic)” should both require a minimum age and explicit consent from a guardian.⁶⁰ The vague obligation for providers to include, for guardians, “mechanisms aimed at managing settings pursuant to Articles 11 and 12,” in combination with the

⁵⁵: *EKA Proposal*, *supra* note 3, arts. 11(1), 14(1)(b).

⁵⁶: *Id.* art. 11(2).

⁵⁷: *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”).

⁵⁸: *Id.* art. 11(2).

⁵⁹: *Id.* art. 11(2).

⁶⁰: *Id.* recital 30.

previous prohibition, 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.⁶¹

If it 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 that brings 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 under-15s. The same goes for geolocation, which means the end of under-15s playing Pokémon Go.⁶² AI firms will need to disable their “memory” function by default unless users verify they are over 15.⁶³ 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.”⁶⁴ Given that this definition anchors on the much wider “AI system” definition, rather than the AI Act’s “general-purpose AI system” definition, and 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. 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 of this, fluffy white 2001 therapeutic soft toy Paro the Seal, arguably the world’s best-known care robot, 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 under-15s, and has no mechanism for discerning who is or is not that age, because it is a soft toy.⁶⁵

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

IV. AWKWARD REALITIES OF AGE ASSESSMENT AND PARENTAL ATTESTATION

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. In certain situations, it relies upon age

⁶¹: *Id.* art. 20(4)(b).

⁶²: 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.

⁶³: *EKA Proposal*, *supra* note 3, art. 14(1)(b).

⁶⁴: *Id.* art. 3(5)(c).

⁶⁵: *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).

verification tools, which connect to a very specific European regime about identities and proof.⁶⁶ It also relies upon parent and guardian attestation tools, to be specified in a delegated act. All of these have complexities and oversights which 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 either be powered by age verification or age estimation. 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. Age verification refers to 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. Age estimation refers to a probabilistic inference of age from various signals which vary massively in quality and reliability. Even where age estimation functions, it does much better at distinguishing small children from adults than it does at distinguishing between adults and adolescents.

The broad structure of the EKA Proposal is that age *verification* is a requirement for social networks' and video platforms' delayed account creation provisions. Such age verification technologies must be certified by an EU certification scheme also seeded by this Regulation. For the design-based obligations, insofar as many of 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.⁶⁷

B. ATTESTATION OF PARENTHOOD OR GUARDIANSHIP

The definition of guardian in the EKA Proposal is "any person holding parental responsibility over a minor pursuant to applicable national law."⁶⁸ The EKA 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."⁶⁹

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 EKA framework is enforced, this either excludes children from digital services, or excludes these carers from the guardian tools. A similar

⁶⁶: 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.

⁶⁷: EKA Proposal, *supra* note 3, arts. 27, 28(1).

⁶⁸: *Id.* art. 3(5)(b).

⁶⁹: *Id.* recital 15; Council Regulation (EU) 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.

situation happens 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.⁷⁰ The EKA 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, exercising rights coming from some position of guardianship or responsibility, could best practically help the minor with their digital life. 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.”⁷¹

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 in the event of a conviction for violence against the other parent.⁷² No mechanism or obligation for the service provider to keep the provision up to date is provided in the Proposal, nor for the child or any other actor to trigger a need to reassess parental responsibility. Legal orders may restrict the exercise of parental responsibility without removing it, but these orders are unlikely to specify the online supervision of children as a specific item, leaving uncertainty, even were the data to be there, 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.

Many Member States simply do not have reliable digital data sources for even conventional guardianship situations, let alone complex ones. Several Member States lack even basic infrastructure for simple parental attestation. For example, in Ireland, unmarried fathers sign a statutory declaration to obtain joint guardianship with the mother. When this is used, this witnessed form is the *only* proof of such guardianship existing; there is no central registry for these statutory declarations.⁷³ German population registers and French civil status records are heavily decentralized to thousands of authorities, and are not considered authoritative on custody orders. The Proposal states that Member States must provide “appropriate alternative procedures where parental responsibility cannot be demonstrated through standard civil status documentation.”⁷⁴ For many Member States, this will be an enormous, potentially expensive, and largely manual undertaking.

Even if verified documents were provided, the same verification will 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.”⁷⁵ 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 European children live in a Member State that does not recognize their parentage for all purposes, and its proposed solution, the European Certificate of Parenthood, has at the time of writing never escaped the Council.⁷⁶ Given the

70: Josep Ferrer-Riba, *Parental Responsibility in a European Perspective*, in *EUROPEAN FAMILY LAW VOLUME III* pp 284–310 (Jens M Scherpe ed., 2016), <https://www.elgaronline.com/edcollchap/9781785363047.00017.xml>.

71: EKA Proposal, *supra* note 3, 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.

72: GREVIO, *Thematic Perspectives on the Implementation of the Istanbul Convention*, COUNCIL EUR. 57 (2025), <https://rm.coe.int/thematic-perspectives-on-the-implementation-of-the-istanbul-convention/1680b4a2e3>.

73: Treoir, *Guardianship Information*, TREOIR (2026), <https://treoir.ie/information/guardianship-information/>.

74: EKA Proposal, *supra* note 3, art. 31(3).

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

76: Proposal for a Council Regulation on Jurisdiction, Applicable Law, Recognition of Decisions and Acceptance of

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?⁷⁷ 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.

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.⁷⁸ Yet the service provider, when accepting such declarations, has to both “make reasonable efforts to verify that the adult making the self-declaration is exercising parental responsibility” while also undertaking the verification “in a privacy-preserving manner and 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.”⁷⁹ 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. They may have to verify they are 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 not have to do much more than that.

C. AGE ASSURANCE... WITHOUT DATA?

The Digital Services Act, 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.”⁸⁰ The proposed EKA “specifies and complements”

Authentic Instruments in Matters of Parenthood and on the Creation of a European Certificate of Parenthood, COM (2022) 695 final (Dec. 7, 2022) [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) (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 (2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022SC0391>.

⁷⁷: Consolidated Version of the Treaty on the Functioning of the European Union, arts. 81(3), 114, 2016 O.J. (C vol 202) 47.

⁷⁸: EKA Proposal, *supra* note 3, art. 26(1)(c).

⁷⁹: *Id.* art. 26(2), (4).

⁸⁰: Digital Services Act art. 28(3).

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.”⁸¹ 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 proposed EKA 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 means additional to what the platform already processes; however, while the EKA 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.⁸² 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 proposed EKA 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.”⁸³ It also states, somewhat grammatically questionably, that “[a]ny age assurance measure shall be zero knowledge proof.”⁸⁴

All this falls apart when the rest of the Regulation, or indeed the field of privacy engineering, is considered. A zero-knowledge proof is a cryptographic protocol that demonstrates a statement without revealing the process of proving that statement. Physical identity cards can be set up, for example, that 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 things like facial imagery, voice and video, document scans, or the patterns of typing or service use.⁸⁵ Such mechanisms are not mentioned in the Regulation, 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.⁸⁶ 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.⁸⁷

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 Regulation. 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

⁸¹: *EKA Proposal*, *supra* note 3, art. 1, recital 6.

⁸²: *Id.* art. 2.

⁸³: *Id.* art. 28(1).

⁸⁴: *Id.* art. 28(3).

⁸⁵: See generally Sas & Mühlberg, *supra* note 66. 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.

⁸⁶: *EKA Proposal*, *supra* note 3, art. 32(2)–(3), recital 61.

⁸⁷: *Id.* recital 61.

identification of the recipient nor locate, track, target, advertise to or profile recipients for any purpose,”⁸⁸ providers should, somehow, “limit the creation, by minors, of secondary accounts aimed at circumventing safety by design measures.” 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 even impossible, tensions, and asks even the smallest social networks or video platforms to solve them.⁸⁹

D. WHEN IT GOES WRONG

Many of these 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. Other EU instruments reflecting on 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, while the only conditions the Proposal places on such processes are that they should be “effective” and “free of charge.”⁹⁰ Those excluded from a service under the proposed EKA have no recourse to a regulator to challenge an individual decision (rather than general non-compliance),⁹¹ or access to an out-of-court dispute settlement body. This is questionable under European law; such decisions would likely be classified as a significant, solely automated decision taken on the grounds of Union law.⁹² This requires that same law to “[lay] down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests.”⁹³ A complaint-handling mechanism is a procedural obligation. It is not a substantive safeguard.

E. OR JUST TIMES OUT

Such recourse will be needed at scale after a six-month period from the Regulation entering application, where any account on any covered provider “in relation to whom the age cannot be established” must be disabled.⁹⁴ 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 blindly self-attestation.⁹⁵ 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

⁸⁸: *Id.* art. 28(1).

⁸⁹: *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.

⁹⁰: *Id.* art. 29(5); *cf.* Digital Services Act art. 20; Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work, art. 10, 2024 O.J. (L 2831) 1.

⁹¹: *EKA Proposal*, *supra* note 3, art. 21.

⁹²: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 22(2)(b), 2016 O.J. (L 119) 1.

⁹³: *Id.* art. 22(2)(b).

⁹⁴: *EKA Proposal*, *supra* note 3, art. 6(4).

⁹⁵: *Id.* arts. 30(3)(a), 20(7), 26(5).

age verification solution for citizens and residents.⁹⁶ Member States also, for the Regulation 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 is 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 seems disingenuous. The Digital Services Act had over a year for its main provisions; the AI Act, following the Omnibus, is set for three years.

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.⁹⁷ These, too, face significant practical and interpretive problems.

A. 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 upon disproportionately vulnerable categories of children. Expert researchers who focus on the lives of such children will surely be able to provide many more examples than I can. But even I can think of a huge number of situations which this Proposal is ill-prepared to respond to.

The structure of the aged 13–15 social network and video platform derogations places the guardian in a significant position of power over the child, for example, able 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 the guardian having access to “monitoring tools,” such as flagging “repeated searches” the child makes about harmful topics.⁹⁸ It is welcome that the law proposes that 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.⁹⁹ It should not be the case that parents have the ability to block, or even monitor, attempts for their child 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 lose a parent or are orphaned; they are taken away from guardians while legal proceedings determine guardianship. Parents 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

⁹⁶: *Id.* art. 31(5).

⁹⁷: *Id.* arts. 3(5)(p), 20.

⁹⁸: *Id.* recital 43.

⁹⁹: U.S. Dep’t of Health & Hum. Servs. *Child Maltreatment 2024*, ADMIN. FOR CHILD. & FAMILIES (Jan. 16, 2026), <https://acf.gov/cb/report/child-maltreatment-2024>; Office for National Statistics, *Abuse During Childhood in England and Wales: March 2024*, OFF. FOR NAT’L STAT. (Nov. 5, 2025), <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/abuseduringchildhoodinenglandandwales/march2024>.

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.¹⁰⁰ 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 and to ignore this is to ignore, and even exacerbate, the struggles of an enormous number of children throughout Europe.

B. 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.¹⁰¹

This paragraph needs some unpacking. First, there is a strange overlap between two of the main threshold-based digital laws passed by the EU in recent years. The “very large online platforms” (VLOPs) of the Digital Services Act, designed to regulate the design and moderation of large online platforms, are referred to at the start of the provision. Yet at the end, Article 6 of the Digital Markets Act, designed to temper the economic power of large firms, is referred to — an obligation that specifically only applies to a handful of designated “gatekeepers.”¹⁰²

It is unclear whether this is intended to mean that only entities that were *both* VLOPs and gatekeepers would be addressed under this part of the Proposal, or whether it applies to all entities that qualify as VLOPs. A 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 imported wholesale — Article 6 contains a whole range of provisions. It may just be a reminder that Article 6, too, extends to the guardian tooling, in cases where Article 6 usually applies. Yet if we adopt such a cross-over reading and look for firms that are the intersection, 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 to only apply to operating systems and virtual assistants, not social networks or similar. 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 this to apply *mutatis mutandis*, it should have said so — better, it should write out what it actually means as an obligation that makes cogent sense.

Perhaps instead we should assume an all-VLOPs reading, disapplying the DMA scope and applying Article 6, perhaps even generously narrowing it to Article 6(7), *mutatis mutandis*. This is supported by the phrasing of the relevant recital.¹⁰³ Yet this too brings enormous confusion.

¹⁰⁰: EKA Proposal, *supra* note 3, recital 18.

¹⁰¹: *Id.* art. 20(5).

¹⁰²: Digital Markets Act art. 3; Digital Services Act art. 33.

¹⁰³: EKA Proposal, *supra* note 3, 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.”).

Which parts of Article 6 apply to VLOPs? Who enforces them, and using what powers, given that the DMA powers extend only to enforcement against designated gatekeepers?¹⁰⁴

In any case, connecting this to the DMA is a lazy and conceptually confusing way to achieve policy aims. The relevant DMA interoperability provision is intended to allow firms to limit the ability to create privileged ecosystems, such as pushing customers to buy a wearable device because it is the only one that works with their phones.¹⁰⁵ Placing a regulatory obligation on a firm to undertake a certain practice does not necessitate that this regulatory obligation should therefore become a market. It is much clearer that the obligation is designed to make things easier for guardians to manage their child’s online life across multiple services in one place, and 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 their trustworthiness? Or can they apply security criteria, given that this is very sensitive data concerning children? Recent interoperability provisions concerning content data have had such a structure for a reason.¹⁰⁶ No clear obligations, such as those that apply to providers to strictly prevent processing of personal data other than for the purposes envisaged in the Regulation, apply to these third parties.

C. 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 children, including explicitly by stalking and surveilling the victim via children’s devices.¹⁰⁷ 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.¹⁰⁸

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.¹⁰⁹ Yet nowhere in the Proposal is there an obligation to protect adults whose

¹⁰⁴: Digital Markets Act art. 29(1).

¹⁰⁵: *Id.* recital 55.

¹⁰⁶: *Id.* art. 7(9).

¹⁰⁷: See Anniina Kaittila et al., *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 NEGL. 107878, 6 (2026).

¹⁰⁸: 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/>; Magdalene Taylor, *The Kinksters Using HR Software to Let Others Control Their Private Info*, MEL MAG. (2022), <https://melmagazine.com/en-us/story/anydesk-teamviewer-blackmail-kink-cyber-domination>; Sexual Health Alliance, *Turn on: Technical Domination*, SEXUAL HEALTH ALLIANCE (Dec. 26, 2023), <https://sexualhealthalliance.com/nymphomedia-blog/turned-on-technical-domination>.

¹⁰⁹: Rahul Chatterjee et al., *The Spyware Used in Intimate Partner Violence*, in 2018 IEEE SYMPOSIUM ON SECURITY AND

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 on 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.¹¹⁰ 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 need to 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.¹¹¹ This Article is more focused on the textual issues in the law than 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.”¹¹² They must however do this at the same time as they “ensure 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.”¹¹³ 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.”¹¹⁴ These pull in somewhat opposite directions: giving priority to specific user preferences inherently narrows the possibility of diversity here, and that primacy limits the ways in which filter bubbles might be tackled through injecting content that overrides narrow preferences. There are genuine

PRIVACY (SP) pp 441–458, 9 (2018).

¹¹⁰ Kautila et al., *supra* note 107, at 6.

¹¹¹ See, e.g., Ari Waldman, *Disorderly Content*, 97 WASH. LAW REV. 907 (2022); Zahra Stardust et al., *Mandatory Age Verification for Pornography Access: Why It Can’t and Won’t “Save the Children”*, 11 BIG DATA SOC. 20539517241252129 (2024).

¹¹² EKA Proposal, *supra* note 3, art. 10(2)(a).

¹¹³ *Id.* art. 10(2)(d).

¹¹⁴ *Id.* recital 28.

questions about whether the Proposal does wish to bring “rabbit holes” within scope. This is clearly a tension, as while they get three lengthy sentences in the recitals, they are not referenced at all in the operative articles, beyond the emphasis on repeated encounters with harmful content being undesirable.¹¹⁵ 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 Regulation 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.”¹¹⁶ 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.¹¹⁷ In contrast to the regime in the United States,¹¹⁸ 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.

The claim that nothing in the Regulation 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.¹¹⁹ It 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.¹²⁰ Unlike in the case 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 specific safeguards, and the 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.¹²¹ If a legal obligation such as that laid out in the Proposal is accepted as not comprising general monitoring, then it is a claim that the general monitoring prohibition does not prohibit detection-by-design that constitutes independent assessment of content, despite having equivalent functional effect to a previously prohibited requirement.

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 recom-

¹¹⁵: *Id.* art. 10(2)(d).

¹¹⁶: *Id.* recital 7.

¹¹⁷: Digital Services Act art. 8.

¹¹⁸: 47 U.S.C. § 230.

¹¹⁹: *EKA Proposal*, *supra* note 3, art. 10(2)(d).

¹²⁰: Case C-70/10, *Scarlet Extended v. SABAM*, ECLI:EU:C:2011:771 (Nov. 24, 2011); Case C-360/10, *SABAM v. Netlog*, ECLI:EU:C:2012:85 (Feb. 16, 2012).

¹²¹: Case C-401/19, *Poland v. Parliament*, ECLI:EU:C:2022:297 (Apr. 26, 2022).

mender 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.¹²² 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

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 for putting in front of a legislative process. This Proposal is not ready for that. The thicket of definitions 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 law’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 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.¹²³ 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.

The Commission should withdraw this Proposal and reissue a workable and realistic text.¹²⁴ 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.

¹²²: *WebGroup Czech Republic & Others*, ECLI:EU:C:2026:492, ¶ 112; *Case C-421/24, AGCOM v. Google*, ECLI:EU:C:2026:592, ¶ 38 (July 16, 2026).

¹²³: *EKA Proposal*, *supra* note 3, art. 28(3).

¹²⁴: *Case C-409/13, Council v. Comm’n*, ECLI:EU:C:2015:217, ¶ (confirming the Commission’s power to withdraw proposals) (Apr. 14, 2015).