AMENDED Exhibit 989

PLAINTIFFS' OMNIBUS OPPOSITION TO DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT

EXPERT REPORT OF TIM ESTES

May 16, 2025

TABLE OF CONTENTS

I. INTRODUCTION

1. My name is Tim Estes. For over twenty years, I have developed and built critical software systems for high-stakes environments using cutting-edge technologies. I have applied these skills in a variety of contexts including, most pertinently, designing and building an online platform intended for children. I was asked by the Plaintiffs' Steering Committee in this case to evaluate whether the Defendants' social media platforms, as designed, were or are reasonably safe for children; to evaluate whether the Defendants implemented adequate age verification and parental controls on their platforms; and to determine whether the Defendants could have, and should have, implemented safer alternative designs. This report contains my opinions and conclusions.

II. QUALIFICATIONS

2. I have spent my career developing safe and secure digital platforms for a wide range of clients. Those platforms have been used by the U.S. intelligence community (to identify and locate terrorists), tier-1 banks (to identify insider trading, collusion, and market manipulation), healthcare systems (to identify possible cancer cases), and law-enforcement agencies (to identify child sex trafficking).

3. I have also developed an online platform (AngelQ) that is specifically designed for children and that utilizes a variety of technologies to keep children safe online. In developing that platform, I conducted an extensive review of the safety systems used by other platforms that target children, including social media platforms and video game platforms. That research led our team at AngelQ to implement a number of safety features that were readily available to, but not used by, the defendants.

4. Through my experience developing these platforms, I have become intimately familiar with the digital safety and security technologies available to companies like the Defendants. In particular, I have a deep understanding of how natural language processing (NLP) and artificial intelligence (AI) systems work; how those systems have been deployed to solve a variety of difficult problems; and how they can be made robust and secure, even when deployed at scale. In other words, I know what digital security features are feasible and what are not, and how that has changed over time. I also have become intimately familiar with principles of user interface design, and the impact interface design and default settings can have on user behavior. All of this experience informs my opinions about how existing technologies could have (and should have) been used by the defendants to address the harms presented by their social media platforms. It also informs my opinions regarding claims by the defendants that certain safety systems would not be workable at scale or would create unreasonable data security risks. This section summarizes my experience.

Academic Background and Early Innovation Experience

5. I earned a Bachelor of Arts in Philosophy from the University of Virginia in 2001, with a concentration in the philosophies of language and mathematics. My undergraduate work provided the conceptual scaffolding for the first generation of self-learning language models that I developed through Digital Reasoning, a company I founded.

6. My university research focused on the intersection between formal systems (symbolic logic and programming languages) and informal systems (natural language and communication). My conjecture was that there was inherent order in informal systems that could be abstracted if properly observed, and that order could be found in variances (statistical stabilities) in the usage of language. Discovering this order could allow formal systems (computers that could rewrite their own code) to be constructed dynamically from understanding natural language communication.

7. In 2000, while still a student, I incorporated Digital Reasoning Systems and began formalizing algorithms that could infer semantic relationships directly from raw text without manual ontologies through examination of statistical co-occurrence patterns – first between documents and later between concepts and entities inside those documents.

8. Within a year the company secured its first contract in support of Army Intelligence and began to be utilized to turn basic keyword search systems into much more powerful entity-oriented analytics systems.

Digital Reasoning: Building an Industry Standard

Validation from Industry Leading Firms

9. As Chief Executive Officer of Digital Reasoning, I guided the company through six institutional rounds of financing, raising more than $120 million from investors whose due-diligence standards are among the most exacting in the world, including Goldman Sachs, Nasdaq Ventures, Barclays, HCA Healthcare, and In-Q-Tel. The participation of these companies required audited information-security practices, demonstrable model robustness, and repeatable deployment methodologies – foundational elements that continue to inform my view of responsible digital platform governance. As outlined below, we were an early pioneer in developing safe, secure platforms that utilize artificial intelligence to solve a wide range of complex problems, without compromising security.

Operational Deployment in National Security

10. Digital Reasoning's flagship platform, **Synthesys**, was first fielded by the U.S. Army's National Ground Intelligence Center in 2004. Deployed in support of forward-operating networks, Synthesys fused multiple streams of collected intelligence to locate safe-houses, courier routes, and improvised-explosive-device cells across Afghanistan and Iraq. By automatically linking fragments of multilingual chatter to time-and-place intelligence, the software enabled analysts to

surface lethal threats hours or days sooner than was previously possible. This become foundational to the U.S. Army's "G2 Way Ahead" that moved tools from basic search into entity-based analytics systems. After this technology proved successful, our work expanded to building similar platforms for other national security agencies.

"Wall-Street-Grade" Communications Surveillance

11. Beginning in 2012, Digital Reasoning adapted its unstructured data analytics technology for the financial-services sector, enabling global banks to monitor millions of internal e-mails, chat messages, and voice calls for signs of insider trading, collusion, market manipulation, or misconduct. Digital Reasoning was the first Natural Language Processing (NLP) system built with enough security and scale to read all of the most sensitive messages inside highly secure financial services organizations, including UBS. The platform's capacity to understand "trade jargon" and other nuanced natural-language context in near real time became a de facto standard for regulatory technology and earned widespread adoption.

Thorn Spotlight — Rescuing Trafficked Children

12. In 2015, I partnered with Thorn, a non-profit founded by Ashton Kutcher and Demi Moore, to create **Spotlight**, a technology platform that mines escort advertisements and social-media postings to surface indicators of child sex trafficking. Digital Reasoning contributed entity-resolution, image-matching, and linguistic-harm-scoring components that compress what used to be weeks of manual cross-referencing into minutes. Spotlight at one point indexed over 100 million escort ads online – primarily from BackPage. Our technology was able to process those ads and decide, based on multiple factors (including the language used by the poster), whether the individual was probably a minor. By 2018, Spotlight had been credited with identifying 6000+ children being trafficked online and 6500+ child sex traffickers across the country. This technology has been used in all 50 States by over 5,000 law enforcement agencies at the local, state, and federal levels. Spotlight is still in widespread use today and has since been credited by law-enforcement agencies with identifying over twelve thousand at-risk minors and helping dismantle numerous trafficking networks across North America.

Healthcare and Public Safety Applications

13. Recognizing that identical language technology could accelerate clinical-care pathways, in 2015, I launched a healthcare division that later spun out as Azra AI. The system we developed continuously triages radiology and pathology reports, flagging cases of likely malignancy and pushing actionable summaries to nurse navigators. Across hundreds of hospitals the solution has reduced time-to-treatment for cancer patients by days, further demonstrating that stringent privacy controls and high-stakes accuracy can coexist in production AI. It was and is another way that the platforms I have developed have saved lives and served the human good.

Protecting Children Online (AngelQ AI)

14. After Digital Reasoning Systems was acquired in 2020, I began focusing on developing AngelQ, an online platform for children of all ages that is designed around safety from the ground-up. In the course of developing AngelQ, I studied the safety systems used by other digital platforms that serve children, including social media and videogaming platforms. I also studied the harmful effects of features designed by social media companies to keep users, including kids, engaged for as long as possible, leading to problematic and addictive use of their platforms.

15. Through my research, I discovered that numerous features of these platforms take advantage of unique susceptibilities of children, causing unnatural and unhealthy behaviors. Those features, which are discussed in greater detail below, are designed by some of the brightest minds in the technology field and make use of sophisticated technology, but do so in ways that harm, rather than protect, children. This form of exploitation was perhaps less visible than the child sex trafficking that I addressed with Thorn, but no less insidious.

16. AngelQ takes a radically different approach. To develop the platform, I recruited some of the people who had helped build Thorn to ensure AngelQ was built the right way from the beginning. AngelQ incorporates many safety features that have been commercially available or technologically feasible for years, but that the defendants have not implemented, waited to implement, or implemented ineffectively. For example:

- We use a clear, parent-initiated sign-up process that ensures parents (or guardians) have consented to their child's use of the platform ("Verifiable Parental Consent" or VPC). Specifically, we use a credit card charge to confirm that the individual creating an account is an adult, so that minors cannot easily access the App without an adult's permission. Once the adult has created an account, the adult must provide the child's age and consent to the child's use of the platform, and to AngelQ's collection of data from the child. This system is fully compliant with the Children's Online Privacy Protection Act (COPPA).

- AngelQ is a subscription service. There is no advertising on the platform of any kind. While AngelQ's 3rd party streaming integrations with Netflix and Disney+ can use their ad-supported platform, if the parent selects the Kid profile in either, they will see no ads. We use an embedded YouTube player that also does not have ads.

- Perhaps most importantly, we exclude from our platform features frequently used by social media companies that encourage excessive or addictive use, such as infinite scroll, autoplaying of videos, push notifications and gamification. As an example, when a kid finishes a video in AngelQ (such as a 10/20min YouTube video), the video stops at the end, and no additional videos are "autoplayed" or recommended.

- AngelQ's Parent Portal allows parents to see what their children are exploring online, and alerts parents when a child searches for sensitive topics. It also has simple-to-use parental controls that allow parents to limit time spent on the application, including a first-of-its-kind texting capability for parental control and screentime management. Essentially, a parent can tell AngelQ via text that the child needs to get off their device in a certain window of time and then AngelQ starts a countdown/clock on the device and locks the applications when that time limit is hit.

- AngelQ tracks a number of impact metrics to ensure that the platform's features are not contributing to problematic use. For example, we track whether or not AngelQ is helping the child manage screentime better. While the parent can override this, we have healthy limits set as defaults for AngelQ usage.

- Our system minimizes data collection – we aim to store only the child's questions and the system's answers, actively avoiding personal details wherever possible.

- Notably, though AngelQ primarily runs on modern AI tech (like Large Language Models, or LLMs), because of the safeguards that AngelQ has put in place, Apple approved it to run in the App Store under the "Kids" (4+) section. It is one of, if not the, first AI/LLM driven app that has obtained such approval.

17. My work in this field has been driven by stories of severe harms that children have experienced online. For example, in February of 2022, I encountered the case of Nylah Anderson, a 10 year-old girl that took her own life trying to emulate a video ("the blackout challenge") that was served up to her on TikTok by the "For You" algorithm. I was outraged as I understood how easily basic safeguards could have prevented such a tragedy.

18. My research and work on the development of safe platforms for kids has revealed that there are serious risks to kids using social media and of using AI to enhance engagement with kids. I have been very public about those concerns. In April of 2024, I wrote a piece for Newsweek called "If Social Media Is a 'Digital Heroin' for Today's Youth, AI Will Be Their Fentanyl." I have also supported efforts like the Kids Online Safety Act (KOSA) to put in place essential safety standards and an explicit duty of care to keep kids safe online.

Advisory Role with Companies in the Defense and Regulatory Industry

19. In addition to my work with AngelQ, I also have an advisory role supporting organizations and companies that employ AI technology across military, security, and compliance uses:

- **MissionLink (United States)** — I serve on the Advisory Board, mentoring growth-stage founders whose products address intelligence, defense, and space missions.

- **Mission Link UK** — I have supported the sister program to the United Kingdom since its kickoff in 2023 and joined their Advisory Board in 2024, working with cabinet-level departments to accelerate the adoption of AI and other high tech capabilities in support of enhanced security for one of our most critical allies.
- **Portfolio Advisory** — I directly advise several defense-oriented and regulatory-oriented start-ups including Replica Cyber, which offers a leading secure-environments-as-a-service platform to defense and industry. I also advise Shield FS – a leading company in the communication surveillance and intelligence business supporting some of the largest financial services companies in the world.

Intellectual Property Portfolio

20. My deep understanding of AI technology is further reflected in my portfolio of patents, which cover inventions in unsupervised language learning, knowledge-graph construction, real-time communications surveillance, and machine-learning life-cycle management. These patents reflect my significant contributions to the field throughout the maturation of AI, from early technical discoveries to the operation of modern systems.

21. The United States Patent and Trademark Office has granted the following patents, all of which list me as an inventor:

Patent No.	Year Issued	Title (abridged)	Principal Contribution
12,106,078	2024	Rapidly Building, Managing, and Sharing Machine-Learning Models	End-to-end life-cycle automation for enterprise ML governance
12,026,455	2024	Construction, Maintenance, and Improvement of Knowledge Representations	Continual-learning methods for dynamic knowledge graphs
11,640,494	2023	Construction, Maintenance, and Improvement of Knowledge Representations	High-volume entity-relationship analytics with feedback optimization
10,878,184	2020	Construction, Maintenance, and Improvement of Knowledge Representations	Distributed annotation and active-learning workflow for NLP
10,049,162	2018	Knowledge Discovery Agent System	First production deployment of unsupervised semantic clustering at petabyte scale
9,699,192	2017	Construction, Maintenance, and Improvement of Knowledge Representations	Real-time update architecture for compliance analytics

9,348,815	2016	Construction, Maintenance, and Improvement of Knowledge Representations	Adaptive schema evolution for multichannel communications data
9,189,749	2015	Knowledge Discovery Agent System	Industrial-scale inference engine with on-the-fly concept learning
7,249,117	2007	Knowledge Discovery Agent System and Method	Foundational unsupervised language-model patent underpinning Synthesys

In Summary

22. My career evidences a singular focus: developing and implementing reliable, secure, cutting-edge software systems that help keep people safe. These are "mission oriented" use cases – the platforms and/or practices I have built are now embedded across intelligence agencies, Fortune 100 banks, public-safety organizations, healthcare networks and online platforms for children. These experiences – paired with a validated portfolio of patents – equip me to offer authoritative, technically rigorous, and practically grounded expert opinions concerning the design, use, and oversight of advanced digital technologies.

23. A copy of my current curriculum vitae and a list of all publications authored by me in the past 10 years is attached as **Exhibit A.**

24. Materials I considered in forming my opinions are identified throughout this report and in **Exhibit B.**

25. A statement of my compensation in this case is attached as **Exhibit C.**

26. A list of my prior testimony is attached as **Exhibit D.**

III. METHODOLOGY

27. In preparing my opinions, I reviewed features of the Defendants' platforms related to child safety, including default settings for child accounts, safety features for children, privacy settings, age verification systems, Verified Parental Consent (VPC) systems, parental controls and warnings systems. In evaluating those features, I looked at documents produced by the Defendants, as well as testimony from current and former employees of the Defendants and publicly available documents. I also conducted research into child safety designs used by other digital platforms directed at children, and drew upon my knowledge and experience from decades of working in digital platform development, including my work for Thorne developing technology to reduce child sex trafficking and my work and AngelQ making a safe online platform for kids. This is the same methodology that I typically use when evaluating digital platforms for companies I am advising, or when developing a digital platform myself.

IV. SUMMARY OF OPINIONS

28. The following opinions detail my conclusions based on my professional training and experience, the relevant standards in the tech industry, the relevant literature, and my extensive review of documents and testimony in this case:

29. As discussed in the reports submitted by Plaintiffs' other experts[1] and confirmed by the U.S. Surgeon General and my own experience and education on these issues, the Defendants' social media platforms can contribute to a wide range of harms in kids, including anxiety, depression, sleep disruption, negative body image, eating disorders, and self-harm, as well as structural changes to the brain. They have also become hunting grounds for predators seeking to sexually exploit children.

30. The Defendants could have (and should have) greatly reduced these harms and risks with technological solutions that were readily available to them. As outlined below, these solutions were technically feasible and in many cases had been implemented by other companies in other contexts. But the Defendants either did not implement them, waited unreasonably long to implement them, or implemented them in ways that were predictably ineffective.

31. **Opinion 1:** The Defendants' platforms, as designed, were not reasonably safe for children. The platforms utilized numerous "dark pattern" design features that contribute to addictive and compulsive use. For children's accounts, the Defendants could have (and should have), disabled features known to cause addictive and compulsive use, as well as features shown to contribute to mental and physical health problems, including (for example) through negative social comparison. The Defendants, moreover, could have (and should have) created strong default privacy settings for children's accounts to limit the ability of sexual predators to contact children and to reduce harassment. The Defendants likewise could have (and should have) implemented systems to track and analyze the harms caused by their platforms, and tested and implemented features for children's accounts that limited those harms. The Defendants, instead, prioritized growth and engagement over safety. The purported safety features they did implement were delayed and frequently designed to fail.

32. **Opinion 2:** Having failed to create a safe environment for children, the Defendants should have implemented systems to help parents and guardians protect children from the potential harms of their platforms. One of the most basic ways to protect children from adult-oriented platforms is a system of age verification and Verified Parental Consent (VPC). This ensures that children or minors under a designated age are not able to set up an account without some form of adult consent and supervision. It also allows the platform to exclude the youngest and most vulnerable children altogether. The Defendants could have, and should have, set up an age verification and VPC

[1] I have reviewed the reports submitted by the following experts on April 18, 2025: Anna Lembke, Dimitri Christakis, Jean Twenge, Kara Bagot, Ramin Mojtabai, Stuart Murray, Drew Cingel, Eva Telzer and Gary Goldfield.

system. In public statements, the Defendants stated that children under 13 are not allowed on their platforms. In practice, however, the Defendants' age verification systems were either non-existent or broken. The Defendants allowed millions of pre-teens to use their addictive platforms and collected data from them without obtaining any form of VPC, in violation of industry standards and regulations.

33. **Opinion 3:** The Defendants' claims that age checks and VPC were not feasible or would have created unreasonable privacy risks are incorrect. Effective, privacy-friendly ways to check age and obtain VPC have been feasible since at least 2010. Methods like credit card checks, secure login systems, and AI-based age estimation were available and proven. Companies in other industries, including video game platform developers and mobile device platform developers, have utilized age verification and parental consent for more than a decade.

34. **Opinion 4:** In addition to requiring parental consent, the Defendants could have (and should have) provided parents and guardians with tools to track and limit their children's use of the platforms. To be effective, these parental controls should have been in place by default, and should have defaulted to the safest setting. The Defendants failed to implement parental controls for years, and when they did finally implement them, they were opt-in, rather than default, and therefore largely ineffective.

35. **Opinion 5:** Stronger, more effective parental control systems were common and technically easy to implement. Xbox, for example, offered time limits by the early 2010s; Netflix Kids profiles allowed parents to limit access to certain features by 2013; Google's own Family Link – applicable to other Google services, but not YouTube – offered robust controls since 2017. Defendants' social media platforms lagged far behind established industry norms for these types of safety features.

36. **Opinion 6:** For parents to provide ***informed*** consent and make meaningful use of parental controls, it is critical that parents be fully informed of the platforms' risks, and understand the precautions that should be taken. Based on my experience and knowledge, the Defendants could have (and should have) informed parents, children and the public about the platforms' potential harms and adequately educated them on how to avoid those harms. Effective warnings systems were technically feasible using both standard 2010-era tools and modern AI. Simple default pop-ups (like health warnings), automatic alerts for excessive and/or problematic use, or AI detecting risky behavior were readily available technologies. In fact, the Defendants used similar tech for ads and engagement.

37. **Opinion 7:** The Defendants have more recently pursued the use of AI technology to further drive engagement despite harms and risks to kids. This includes the use of "companion" chatbots and similar techniques. The Defendants have failed to implement reasonable safeguards for these technologies, showing a continuing failure to focus on safety. Their use of AI to further addict children is likely to unleash an even greater wave of preventable harms.

V. BACKGROUND

A. Overview of Defendants' Platforms

38. The Defendants represent some of the largest and most valuable companies in the world. Their combined market capitalization as of May 2nd, 2025 was ~$3,740 Billion or roughly the GDP of Germany.[2] Their combined revenues were >$700 Billion in FY 2024 and they had approximately $200B in income.[3] The size of these companies, and the resources available to them, are relevant to understanding the feasibility of the safer alternative designs that are discussed below.

39. **Meta Platforms, Inc.** Meta operates two of the largest social-networking services in the world – Facebook, launched in February of 2004, and Instagram, introduced as a mobile photo-sharing app in October 2010.[4] Together these apps reach roughly 3.07 billion and 2 billion monthly active users (MAUs) respectively, making Meta the largest social-media provider by audience size.[5] The company derives most of its revenue from targeted advertising delivered across Facebook, Instagram, Messenger, and related services.[6]

40. **Snap Inc.** Snap is the owner of Snapchat, a mobile-first messaging and multimedia application created in 2011.[7] Snapchat emphasizes ephemeral "Snaps," augmented-reality Lenses, and user-generated Stories. It now has well over 100 million users in the United States and

[2] Meta: https://companiesmarketcap.com/meta-platforms/marketcap/; Snap: https://companiesmarketcap.com/snap/marketcap/; Alphabet: https://companiesmarketcap.com/alphabet-google/marketcap/; TikTok: https://www.statista.com/statistics/1324424/tiktok-brand-value/; Germany: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DE.

[3] *Id.*

[4] "Facebook Launches" (October 29, 2019), https://www.history.com/this-day-in-history/february-4/facebook-launches-mark-zuckerberg.

[5] "What are the top social media platforms in the world?" (last updated March 11, 2025), https://soax.com/research/top-social-media-platforms.

[6] "Meta Earnings: Record Profits, Sales as Ads Stay Robust During Zuckerberg's Year of Efficiency"(October 25, 2023), https://www.forbes.com/sites/dereksaul/2023/10/25/meta-earnings-record-profits-sales-as-ads-stay-robust-during-zuckerbergs-year-of-efficiency/.

[7] "Snapchat: The Biggest No-Revenue Mobile App Since Instagram" (Nov 27, 2012), https://www.forbes.com/sites/jjcolao/2012/11/27/snapchat-the-biggest-no-revenue-mobile-app-since-instagram/.

hundreds of millions worldwide.[8] Snap monetizes its platform primarily through advertising, including Sponsored Lenses, Discover content, and in-app Spotlight media placements.

41. **ByteDance Ltd. (TikTok).** ByteDance's flagship international product, TikTok, emerged from the 2016 launch of its Chinese twin app Douyin and expanded globally after ByteDance's 2018 acquisition of Musical.ly, another social media platform that was integrated into TikTok.[9] TikTok now attracts approximately 1.04 billion monthly active users worldwide, positioning it as the dominant short-form video network outside China.[10] TikTok's revenue is driven by algorithmically targeted video advertising and an in-app creator economy centered on virtual gifts and commerce links.[11]

42. **Google LLC (YouTube).** YouTube debuted in April 2005, and was acquired by Google in October 2006 for $1.65 billion in stock.[12] It hosts both short- and long-form video as well as livestreaming and music content. Today the platform has more than 2.49 billion monthly active users.[13] YouTube's revenue comes primarily from advertising, supplemented by subscription products such as YouTube Premium and YouTube Music.[14]

B. Harms of Defendants' Platforms

43. As demonstrated in the expert reports previously submitted by the Plaintiffs, as noted by the U.S. Surgeon General, and based on my experience and knowledge from studying and working in this area, I understand that the Defendants' social media platforms can contribute to a wide

[8] "Snapchat Statistics" (last updated Jan 3, 2025), https://analyzify.com/statsup/snapchat?utm_source=chatgpt.com.

[9] "TikTok Explained" (Jul 12, 2019), https://www.vox.com/culture/2018/12/10/18129126/tiktok-app-musically-meme-cringe.

[10] "Tik Tok Statistics You Need to Know" (last updated Mar 8, 2025), https://backlinko.com/tiktok-users.

[11] "Tik Tok's Revenue Engine: Decoding How the Video Giant Monetizes Its Platform" (May 7, 2025), https://medium.com/@miracuvesseo/tiktoks-revenue-engine-decoding-how-the-video-giant-monetizes-its-platform-972bed71e105

[12] "Watch Youtube's First-Ever Video as Bizzarre 19-Second Clip with 355 Million Views Uploaded 20 Years Ago Today" (Apr 23, 2025), https://www.thesun.co.uk/tech/34597728/youtube-first-video-me-at-the-zoo-google-karim/.

[13] "Youtube Stats: How Many People Use Youtube?" (last updated Apr 14, 2025), https://backlinko.com/youtube-users.

[14] "Youtube Projected to Surpass Disney as World's Largest Media Company" (Apr 3, 2025), https://www.forbes.com/sites/bradadgate/2025/04/03/youtube-projected-to-surpass-disney-as-worlds-largest-media-company/.

range of harms in adolescents.[15] Those include anxiety, depression, sleep disruption, negative body image, eating disorders, and self-harm, as well as structural changes to the brain. Because these platforms have massive user bases, these harms can affect millions (if not tens of millions) of kids every year.

44. These harms are most severe among kids who spend excessive time on the Defendants' platforms – something the platforms are designed to encourage. Features like "infinite scroll," autoplaying of videos, push notifications, ranking algorithms, gamification (*e.g.*, Snapstreaks) and ephemeral content all are designed to make the platforms more addictive.[16] These and other addictive features of the Defendants' platforms are discussed in detail in Opinion 1 below.

45. The Defendants' testimony and internal documents demonstrate this. For example, Meta personnel discussed infinite scroll, autoplay and push notifications as part of its platforms' "'addictive'-like design" and "dark pattern."[17] ("Dark patterns are user interface elements that can influence a person's behavior against their intentions or best interests."[18])

46. TikTok documents similarly refer to "Infinite scroll, video auto-play, and constant notifications" as "some of the powerful coercive design tactics that we are realizing tend to benefit companies and advertisers more than users."[19] Snap documents discuss how Snapstreaks "have tapped into some mass psychosis where 17 million people must keep the streaks going."[20] YouTube documents reference "autoplay" as a feature that "encourage[s] binge-watching," noting that such excessive watching "is related to addiction."[21]

---

[15] *See generally* Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory (2023) (hereinafter, "Surgeon General's Advisory"); Apr. 18, 2025 Expert Report of Anna Lembke; Apr. 18, 2025 Expert Report of Dimitri Christakis; Apr. 18, 2025 Expert Report of Jean Twenge; Apr. 18, 2025 Expert Report of Kara Bagot; Apr. 18, 2025 Expert Report of Ramin Mojtabai; Apr. 18, 2025 Expert Report of Stuart Murray; Apr. 18, 2025 Expert Report of Drew Cingel; Apr. 18, 2025 Expert Report of Eva Telzer; Apr. 18, 2025 Expert Report of Gary Goldfield.

[16] Surgeon General's Advisory at 9.

[17] META3047MDL-044-00108564 at -566; META3047MDL-003-00191207.

[18] "A Comparative Study of Dark Patterns Across Mobile and Web Modalitties" (Oct 2021), https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Gunawan-Pradeep-Choffnes-Hartzog-Wilson-A-Comparative-Study-of-Dark-Patterns-Across-Mobile-and-Web-Modalities.pdf.

[19] TIKTOK3047MDL-006-00327425 at -444.

[20] SNAP6759344.

[21] GOOG-3047MDL-04918852 at Slide 12.

47. Sean Parker, one of the original developers of Facebook, has described how Meta and other platform developers use the addictive nature of these features to maximize time spent on the platforms (which in turn maximizes ad revenues):

> The thought process that went into building these applications . . . was all about how we consume as much of your time and conscious intention as possible. And that means that we need to sort of give you a little dopamine hit every once in a while because someone liked or commented on a photo or a post or whatever. . . . [I]t's exactly the kind of thing that a hacker like myself would come up with, because you're exploring vulnerability in human psychology.[22]

48. YouTube documents similarly indicate that it was part of YouTube's "Vision" to "create an app that is . . . Addictive," meaning "Our app experience should compel users to come back more and more often."[23]

49. Children are particularly susceptible to these tactics.[24] Meta, for example, in an internal document about marketing to teens, explains some of the reasons why:

> **Teen brains are much more sensitive to dopamine**, one of the reasons that the risk of drug addiction is higher for adolescents and it's the same thing that keeps them scrolling and scrolling. Due to the immature brain, **they have a much harder time stopping** even though they want to – our own product foundation research has shown **teens are unhappy with the amount of time they spend on our app**.[25]

50. Aside from addiction and mental health issues, the platforms present other significant risks to children as well. For example, they have become hunting grounds for predators seeking to sexually exploit children. The Defendants' platforms facilitate that in a number of ways, by (for

---

[22] Zuckerberg Dep. at 53:16-54:17 (quoting video recording of Sean Parker).

[23] GOOG-3047MDL-00767071 at Slide 10.

[24] *See, e.g.*, Surgeon General's Advisory at 5 ("Because adolescence is a vulnerable period of brain development, social media exposure during this period warrants additional scrutiny."); Apr. 18, 2025 Expert Report of Drew Cingel, Ph.D. at 20-26; Apr. 18, 2025 Expert Report of Dimitri Christakis, M.D., M.P.H. at 36-41; Apr. 18, 2025 Expert Report of Stuart Murray, Ph.D. at 34; Apr. 18, 2025 Expert Report of Eva Telzer, Ph.D. at 33-45; Apr. 18, 2025 Expert Report of Gary Goldfield, Ph.D. at 29; Apr. 18, 2025 Expert Report of Anna Lembke, M.D. at 20-22.

[25] META3047MDL-003-00191207 at -215 (emphasis in original); *see also* GOOG-3047MDL-02820161 at p. 5 ("Changes in brain development predisposes young teens to act more impulsively, show a greater tendency towards risk taking, and lead to an increased interest in riskier content").

example) recommending predators to children as potential friends, and by recommending children's accounts to adults – particularly adults who show an interest in that type of account – and then allowing those adults to directly message the children's accounts.[26] As a result, children frequently receive unwanted sexual messages from strangers on these platforms.[27]

51. For example, a survey conducted by Meta found that 13% of children aged 13 to 15 on Instagram reported unwanted sexual advances in just the last seven days.[28] "Most teen girls disclosed receiving 'creepy,' 'weird,' 'sexual,' or 'inappropriate' comments or messages from unknown adult men."[29] Meta has estimated that, in English-speaking markets alone, more than 500,000 Instagram underage accounts receive inappropriate interactions from adults on a weekly basis.[30] Similarly, 4 in 10 TikTok users reported encountering inappropriate content related to minor safety in user-to-user interactions.[31] An internal YouTube presentation shows that 8% of minors reported having a sexual interaction on YouTube, and acknowledges that "predators can begin extorting minors through relationship building on YouTube before moving the conversation off platform."[32] YouTube documents further acknowledge that its attempts to address these concerns "are not working" and "Bad actors continue to evade detection."[33]

52. In more extreme cases, children on these platforms have been tricked into sending nude pictures to an adult stranger; nude pictures have been used by adults to blackmail children (sextortion); children have committed suicide following sextortion; and children have been abducted and sexually abused by predators.[34]

53. Law enforcement and child safety organizations have repeatedly warned that popular apps are used to lure children into inappropriate contact or worse. In the UK, where such crimes are

[26] *See, e.g.*, META3047MDL-020-00271442 ("Our existing classifiers do not work great on short form virality that there is no current mitigation for in the Reels product roadmap – namely, predatory DMs from adults sent to minors who are more easily discovered via their Reels content."); META3047MDL-014-00369785 at 2 (discussing how "bad actors can signal one another and look for and connect with kids and then enter a private messaging thread," creating "one seamless flow of discovery-->connection--->harm.").

[27] *See, e.g.*, META3047MDL-014-00046829 ("On IG there are 32X as many of these (messenger threads with sketchy adults) in the US than on FB")

[28] META3047MDL-004-00015029 at -033, -049.

[29] META3047MDL-074-00164587 at 30-31.

[30] META3047MDL-003-00028214 at -218.

[31] TIKTOK3047MDL-002-00102517, -527.

[32] GOOG-3047MDL-02432112 at 20.

[33] GOOG-3047MDL-00246776 at 14, 15.

[34] META3047MDL-014-00350154; Rothschild Dep. at 314-18; TIKTOK3047MDL-002-00094384 at -400; SNAP5195476.

diligently tracked, over 7,000 instances of online grooming (sexual communication with a child) were recorded in 2023-24 – an 89% increase since 2017. [35] The messaging app Snapchat was the most common platform implicated (used in almost half of those cases), with Instagram, WhatsApp, and Facebook together appearing in a significant share as well.[36] The youngest victim was just five years old – meaning a kindergartner ended up on a platform and in contact with a predator.[37]

54. Snap's own internal research found that about one-third of teen girls and 30% of teen boys that use Snap were exposed to unwanted contact on the platform in 2022, and over half of Gen Z users reported experiencing or knowing a friend who experienced catfishing (*i.e.*, someone using a false identity to develop an intimate online relationship), with a quarter of those incidents involving sextortion.[38] Snap's internal data indicated the company was receiving about 10,000 reports of sextortion per month on Snapchat.[39] One account had 75 separate complaints of grooming filed against it and still wasn't taken down.[40]

55. Many of these harms could be prevented or greatly reduced with technical solutions that were readily available to the Defendants. For example, the Defendants could have (and should have):

- for children's accounts, disabled features known to cause addictive and compulsive use, as well as features shown to contribute to mental health problems through negative social comparison;
- restricted the ability of children to communicate with adult strangers, and made children's accounts private by default;
- combined age verification technology with Verified Parental Consent systems to ensure that minors could not access the platform without their parents' or guardians' knowledge and informed consent;
- provided parents and guardians with ongoing information about their children's use of the products, such as the amount of time spent on the apps and the time of day the apps were

[35] "Online Grooming Crimes Against Children Increase by 89% in Six Years" (Nov 1, 2024), https://www.nspcc.org.uk/about-us/news-opinion/2024/online-grooming-crimes-increase/.

[36] *Id.*

[37] *Id.*

[38] "Attorney General Raul Torrez Files Unredacted Complaint Against Snapchat, Exposing Internal messages that Snap Knowingly Contributed to Harm Amongst Children" (Oct 2, 2024), https://nmdoj.gov/press-release/31302/.

[39] SNAP6827402 at 13.

[40] SNAP0350180.

accessed, so that parents and guardians are alerted to signs of addiction before it gets out of control;

- alerted parents and guardians to potentially dangerous activity by their children, such as sending or receiving messages from adult strangers;
- provided both parents/guardians and children with tools to limit use of the platforms – by, for example, setting firm daily time limits, or restricting use during hours when children should be in school or sleeping – and educating them on those tools;
- provided warnings to ensure that both parents and children were fully informed about the platforms' potential harms and educated on how to avoid those harms.

56. As outlined below, these and numerous other options were technically feasible, and in many cases had been implemented by other companies in other contexts. But the Defendants either did not implement them, waited unreasonably long to implement them, or implemented them in ways that were ineffective.

VI. OPINION 1: DEFENDANTS' PLATFORMS, AS DESIGNED, WERE NOT REASONABLY SAFE FOR CHILDREN

A. Defendants Could Have, And Should Have, Disabled Features Harmful to Children

57. Based on my extensive experience in digital platform design, including my work on platforms intended for children, and my review of the Defendants' platforms and documents, it is my opinion that Defendants' social media platforms (Instagram, Facebook, TikTok, Snapchat and YouTube) were and are not reasonably safe for children as they are designed. Each platform includes a host of features that encourage compulsive and addictive use, create harmful social pressure on children, and unnecessarily expose children to dangers like child predators.

58. Many of these features make use of a design technique known as "dark patterns" to keep children engaged on the platform far longer than is healthy. As noted above, dark patterns are deceptive user interface designs that trick or manipulate users into taking actions they would not otherwise have taken. I am intimately familiar with the mechanism of "dark patterns" from my work on the Kids Online Safety Act (KOSA), which seeks to regulate them, and from my development of AngelQ, which purposefully avoids using dark patterns to negatively influence children.

59. These features could have, and should have, been removed or limited on accounts belonging to minors. The failure to remove or limit these features was not due to any technical challenge, but rather was a decision by the Defendants to favor engagement over safety. Below, I examine several of these features and their safer alternatives:

1. Infinite Scroll

60. The Defendants' platforms each include different versions of a feature known as "infinite scroll." This feature loads new content continuously with no natural stopping point – one can scroll through content indefinitely and never hit the bottom. Its purpose is straightforward: remove the subtle cue to stop that a "bottom of the page" or "end of feed" would normally provide.

61. This feature was pioneered by Facebook in 2010 and has since been integrated into Instagram's main feed as well as its "Reels" and "Explore" features.[41] It is likewise integrated into TikTok; into YouTube's home page and "Shorts" feature; and into Snapchat's "Discovery" and "Spotlight" features.

62. It is well known among digital platform designers that the purpose of this feature is to encourage people to stay on the platform for longer periods of time. The inventor of infinite scroll, [redacted], has described its effect as sprinkling "behavioral cocaine" throughout the interface to keep users addicted.[42] As he testified, "Infinite scroll is an intentional removal of stopping cues so that your brain doesn't wake up to catch up with impulses. So it . . . creates that hypnologic state where you just keep scrolling. Doomscrolling would not really exists without infinite scroll."[43] Former Meta user experience researcher Natalie Troxel likewise testified that she "had concerns based on research I had done and conversations I had had with other people in the company that infinite scroll allowed people to use the product more than they wanted or more than they had intended to and that there not being an end or a point where they've caught up could really exacerbate people's use of or problematic use of the products."[44] The Defendants' own documents likewise discuss how this design hijacks users' self-control and contributes to addictive and problematic use, particularly by children.[45] TikTok executives, for example, have described infinite scroll as "one of many coercive design features that detracts from a user's agency."[46]

---

[41] "How the Invention of Infinite Scrolling Turned Millions to Addiction" (Nov 16, 2020), https://medium.com/design-bootcamp/how-the-invention-of-infinite-scrolling-turned-millions-to-addiction-3096602ef9af.

[42] [redacted] Dep. at 73:13-18.

[43] [redacted] Dep. at 41:16-21.

[44] Troxel Dep. at 71:14-21.

[45] TIKTOK3047MDL-015-00341931 at -167 (internal TikTok document noting that "the risk level of this auto-scroll mode [is] High, **especially for teens . . . due to concerns about screen time addiction**.") (emphasis added); META3047MDL-044-00108564 at -566 (internal Meta document describing "Endless Scroll" as part of its platforms' "'**Addictive'-like design**" and "**dark pattern**") (emphasis added); SNAP0307144, SNAP1393050 ("Not sure what to say about addictive endless scrolling. We already have endless scroll design").

[46] Dep. of Furlong at 87-91.

63. A simple, safer alternative was, and is, readily available: paginate the content or insert natural breakpoints (for example, after a certain limited number of posts, require the user to click "see more"). This is how virtually all online platforms worked prior to 2010.

2. Autoplay Videos

64. Another "sticky" feature Defendants employ is autoplay. Each platform offers a slightly different version, but with similar effects. On YouTube, for example, after one video finishes, the next starts automatically without user input.[47] On TikTok, Snapchat and Instagram, videos play automatically as the user scrolls through their feed. TikTok now has a feature they call "auto-scroll," which immediately goes from one video to the next without even a swipe from the user.[48]

65. Autoplay and auto-scroll drag users into hours of viewing they never consciously chose, which can be hugely profitable for the platforms, but also harmful for children and teens who lack the self-control of adults.[49] YouTube, for example, found the introduction of autoplay to be "the single most impactful launch in YouTube history, with +8% desktop watchtime, +4% overall watchtime increase."[50]

66. YouTube added autoplay as a default feature in 2015;[51] Snapchat added it in 2016;[52] and Instagram added it in 2017.[53] TikTok has used autoplay since its inception.[54] Defendants' own documents discuss autoplay's addictive effects, particularly among children.[55]

---

[47] GOOG-3047MDL-00767071 at slide 26.

[48] Furlong Dep. at 103:13-104:10, 330:1-331:25, 340:14-349:18, 351:3-352:1.

[49] *See* META3047MDL-003-00191207 at 15 ("Teen brains are much more sensitive to dopamine…it's the same thing that keeps them scrolling and scrolling").

[50] GOOG-3047MDL-00767071 at slide 27; *see also* GOOG-3047MDL-04613300 ("The [Autoplay desktop] launch's impact has been huge. Autoplay now generates 16% of YouTube's desktop watch time…").

[51] GOOG-3047MDL-04626757 at 6.

[52] "You Can't Turn Off the Most Annoying Feature in the New Snapchat" (Mar 30, 2016), https://www.businessinsider.com/turn-off-snapchat-stories-autoplay-feature-2016-3.

[53] [redacted] Dep. at 80:2-80:16; META3047MDL-031-00266889 at -909.

[54] TIKTOK3047MDL-084-LARK-03183934 at -940.

[55] *See, e.g.*, META3047MDL-044-00108564 at -566 (describe "Autoplay" as part of Instagram's "'Addictive'-like design" and 'dark pattern'"); GOOG-3047MDL-04918852 at Slide 12 (identifying autoplay as a "trick[] to encourage binge-watching," and noting that "excessive video watching is related to addiction"); TIKTOK3047MDL-153-LARK-07390258 (noting that autoplay benefits advertisers, not users).

67. The safer alternative is exceedingly simple: require users to click a button to play a video. Notably, after years of complaints by parental advocacy groups,[56] YouTube did adopt this safer approach for minors eventually, but not until 2021, more than six years after introducing the feature, and many years after employees raised concerns about it internally.[57] Even then, the restriction applied only to users who were logged in (which is not required to use the platform) and who had identified themselves as under 18 during sign-up.[58] As discussed in more detail below, YouTube did not verify users' ages, and "only a small fraction of those who are actually u18 [under 18 years old] are declaring accurately," meaning this feature affects only a small fraction of teen users.[59]

68. Facebook allows users to turn off autoplay; however, the feature is opt-in – autoplay is turned on by default, including for teen accounts, which makes it far less likely to be used. The other platforms (TikTok, Instagram, Facebook, Snapchat) likewise continue to employ autoplay as a default, despite its known harms (though TikTok has announced it is removing auto-scroll).[60] Facebook, TikTok and Snapchat do allow users to turn off autoplay; however, the feature is opt-in and must be turned on by navigating through menu settings, making it far less likely to be used. Instagram makes autoplay impossible to turn off.[61]

3. Gamification (Snapstreaks, Public Like Counts)

Snapstreaks

69. Another addictive element of the Defendants' platforms are "gamifications." For example, "Snapstreaks," introduced on Snapchat in 2015, count the consecutive days two users send each other a photo.[62] While this may appear to be harmless fun at first glance, streaks quickly turned into a source of anxiety and compulsive behavior for teens.

---

[56] *See, e.g.*, Devan McGuinness, "Youtube Finally Turns off Autoplay for Kids. Here's the Catch", Fatherly (August 16, 2021), https://www.fatherly.com/news/youtube-autoplay-kids.

[57] GOOG-3047MDL-04805860 at 15; GOOG-3047MDL-00874191 at 7; GOOG-3047MDL-04652560 at -75.

[58] *See* James Beser Dep.Vol. II, April 3, 2025, at 676:13-677:9; Reid Watson Dep., March 23, 2025, at 250:23-251:20.

[59] GOOG-3047MDL-04703742 at -742; see also GOOG-3047MDL-01339056 at -071 ("[M]ost actual YT Teens users did not declare themselves between 13-17.").

[60] TIKTOK3047MDL-065-LARK-00819445; META3047MDL-004-00029597.

[61] META3047MDL-004-00029597.

[62] "Snapchat Users are so Upset About Losing Their Streaks That They Email the Company to Get Them Back" (Jul 26, 2019), https://www.businessinsider.com/snapchat-streaks-how-to-get-snapstreak-back-2019-7.

70. A focus group conducted by Snap in 2017, for example, found that for many children, Snapstreaks had "become compulsive behavior, and many users feel they are 'in too deep' to get out of a streak."[63] It further explains that teens feel "strong social pressure to maintain a streak, and breaking a streak can negatively affect personal relationships."[64] Documents describe how users feel "addicted,"[65] and "feel pressured to keep Streaks going," even though they "feel they are no longer exchanging meaningful content." [66] Demonstrating the extreme effect this feature can have on teens, after breaking a Snapstreak, desperate children have emailed Snapchat's CEO begging to have them restored.[67]

71. Some Snap employees noted that streaks were "incentivizing problematic or unhealthy usage by young users."[68] Snap executives said of this addictive effect, "Yeah we seem to have tapped into some mass psychosis where 17 million people must keep the streaks going."[69] Notably, around half of Snapstreaks users are under the age of 18.[70]

72. Snap could have, and should have, turned this feature off for minors. Instead, Snap doubled down, and monetized it. Snap now charges users a monthly fee (approximately $4/month depending on region) for Snap+ accounts, which include the ability to "freeze" or "restore" streaks.[71] Alternatively, users can pay Snap 99 cents to restore an individual streak after it is lost. In 2023, the Snapstreak Restore feature generated $47 million.[72]

73. Notably, Snap has implemented other "gamification" features that fuel addictive and compulsive use of its platforms by kids, including "Snapscores" and "Snap Trophies," both of which reward users with digital prizes for more use of the platform.

Public Like Counts

74. Instagram, Facebook, TikTok and YouTube have implemented gamification features as well. For example, on all four platforms, users are able to "like" a post or video they see, and then

[63] SNAP0029949 at -959.

[64] *Id.*

[65] *Id.*

[66] SNAP0640337 at -341.

[67] SNAP0652599; SNAP0867965; SNAP1117208; SNAP1838156; SNAP0896563.

[68] SNAP0396889.

[69] SNAP6759344.

[70] SNAP2345620 at -621.

[71] "Snapchat+", https://accounts.snapchat.com/plus/plans.

[72] SNAP1937542; SNAP4235765.

the "like count" for the post is displayed publicly, creating essentially a popularity score for the posted content. YouTube also has a "dislike" feature.[73]

75. Teens can become obsessed with receiving likes and anxious when they don't, leading to feelings of inadequacy, pressure to curate perfect images, and fear of social rejection. Research has found that the encouragement of social comparison via likes and like counts can be **as damaging to teen mental health as direct harms like bullying**.[74] Other internal documents from the Defendants confirm that this feature can be harmful to teens, by both encouraging excessive use[75] and causing "negative social comparison," which contributes to feelings of "loneliness" and decreased "life satisfaction" and "self-worth."[76]

76. From a product design standpoint, the remedy was straightforward – the Defendants could have, and should have, **hid like counts** for children's accounts. This would remove the constant public scorekeeping and let teens post or scroll without that pressure.

77. Instagram, notably, implemented an option to hide like counts in 2021 – more than 10 years after its creation. However, users have to opt-in to hide likes, which requires navigating through settings menus; the *default* remains showing the numbers. This ensures the feature will not be widely used – "[i]f a feature is opt-in, **almost nobody will use it.**"[77] In fact, two and a half months

---

[73] GOOG-3047MDL-03014621.

[74] Sandra Knispel, Getting Fewer Likes on Social Media Can Make Teens Anxious and Depressed, University of Rochester (September 24, 2020) https://www.rochester.edu/newscenter/getting-fewer-likes-on-social-media-can-make-teens-anxious-and-depressed-453482.

[75] *See, e.g.*, META3047MDL-003-00191207 at -216 ("DMs, notifications, comments, follows, likes, etc. encourage teens to continue engaging and coming back to the app."). TIKTOK3047MDL-153-LARK-07397425 ("An internal study indicates that 50% of inactive TikTok users cited time management as an issue, 24% reported too many notifications, and 23% reported too much time spent on TikTok").

[76] META3047MDL-020-00082810 at 8; *see also* META3047MDL-038-00000234 at -392 ("I think we can be pretty confident of a causal link between Like counts and social comparison."); [redacted] Dep. at 139:19-142:23, 212:21-213:23 (discussing link between public like counts and negative social comparison); Jayakumar at Dep.at 166:3-166:21 (same); META3047MDL-038-00000234 at -234. GOOG-3047MDL-00204482; GOOG-3047MDL-01208976; TIKTOK3047MDL-021-LARK-00012902; TIKTOK3047MDL-099-LARK-04522629.

[77] Bejar Dep. at 167:15-24 (emphasis added); *see also id.* at 548:16-22 (noting that "teenagersdon't go into settings"); *id.* at 582:3-10 (Q. "What impact would those features of parental supervision have for adoption and effectiveness based on your industry experience?" A. "It would mean that the feature would not be adopted and then as such would not be effective as a safety feature."); Gelwert Ex. 20 ("we keep making tools no one is using because we make it a control"); Gelwert [Rough] Dep. 187:7-9 ("I don't think it's a leap to say that when we provide controls, a lot of times young people don't know that we are offering these features.");

after launch only 2.3% of Instagram posters had turned off the public like count.[78] [redacted][79]

78. TikTok does not offer its users the option to hide either the like counts or the view counts on their own videos. YouTube also does not offer creators the option to hide view counts on their videos, but it does provide them with the ability to hide like counts.[80]

4. Engagement-Driven Algorithms

79. Instead of showing content in simple chronological order, each of the Defendants has implemented algorithmic feeds that seek to increase "engagement" – that is, the feed purposefully shows users what it has determined, through monitoring of the user's behavior and other characteristics, is likely to keep them scrolling or clicking for longer.[81] Instagram and TikTok have had algorithmic feeds since launch, YouTube implemented it's algorithmic feeds in 2011,[82] and Snapchat implemented an algorithmic feed through its discover page in 2017.[83]

80. As the Defendants acknowledge internally, these engagement algorithms can, irrespective of content, encourage addiction and compulsive use.[84] By presenting posts based on calculated

---

TIKTOK3047MDL-098-04111887 at -898 ("I predict approximately zero usage - **anything opt in gets very low usage**.").

[78] META3047MDL-047-01342635 (August 16, 2021); *see also* Meta's Sixth Supp. Resp. to Interrogatory 11 ("Hiding public like counts was implemented as an opt-in feature for all Instagram users on May 26, 2021").

[79] Meta's First Supp. Resp. to Interrogatory 12 (Apr. 17, 2025).

[80] "How to Hide Likes & Dislikes on YouTube Videos" (Mar 9,2020) https://vidiq.com/blog/post/how-to-hide-likes-dislikes-youtube-videos-2019/;a"Video: How to Hide Likes, Dislikes & Comments on YouTube Videos" (Apr 29, 2021); (1); TikTok: Liking, https://support.tiktok.com/en/using-tiktok/exploring-videos/liking.

[81] *See, e.g.*, META3047MDL-047-00706686 ("[T]he algorithm is absolutely tuned to maximize engagement in a maximally empirical, principle-less way. I am not sure that the youth legal people realize this, and that it applies to teens just as much as gen pop. . . so the things contained in the lawsuits are somewhat hard to refute so long as Teens are part of the GVM process.").

[82] "Youtube's New Homepage Goes Social with Algorythmic Feed, Emphasis on Google+ and Facebook" (Dec 1, 2011), https://techcrunch.com/2011/12/01/newyoutube/.

[83] "What Snapchat's Major Redesign and Algorhymic Feed Means for Marketers" (Nov 29, 2017), https://martech.org/snapchats-major-redesign-algorithmic-feed-means-brands/.

[84] *See, e.g.*, TIKTOK3047MDL-060-01111628 at -629 (noting that the "recommendation algorithm" can "lead to minors being in a feedback loop."); TIKTOK3047MDL-002-00064418

interest rather than in chronological sequence, the platforms hook users via unpredictable rewards – the same technique casinos use to encourage compulsive behavior.[85] Algorithms can also drive some children down "rabbit holes" [86] or "filter bubbles,"[87] which can likewise contribute to addictive and compulsive use, regardless of what type of content is shown.[88]

81. Safer alternatives were well-known, and should have been implemented for children's accounts. For example, a **chronological feed** (simply showing the newest posts from friends) avoids exploiting reward psychology. Facebook and Instagram originally used chronological feeds and could have kept that as a default option for teens. At her deposition, Meta user experience researcher Natalie Troxel recalled that, when she recommended returning to a chronological feed, she "was laughed at the first time I brought it up . . . it was just a nonstarter."[89] Troxel was told, "we wouldn't be able to do something like that because it would lower engagement."[90] Meta could also have, for teen accounts, **tuned the algorithms to increase well-being**, rather than to increase engagement. (This capability is discussed in more detail in section VI(C).)

82. In 2021, Instagram added a feature that allows users to temporarily "snooze" algorithmically-generated "suggested posts" on their primary feed for 30 days.[91] This feature allows users to go back to an earlier version of the app that does not use algorithms to capture their attention (other than for advertisements, which still appear in the feed). Notably, the feature is "opt-in" – users have to navigate a settings menu to turn it on, ensuring that few people will use it. Even more tellingly, the tested "snooze" feature was temporary – it was ***impossible*** for users to turn off suggested posts permanently. Thus, if an underage user wanted to turn off suggested posts and managed to navigate the setting menu to "snooze" it, the feature would be turned back on

---

at -418 to -419 (discussing how the recommendation algorithm can send users into "rabbit holes"); SNAP3760712 at -713 ("[I]f we want to increase time spent in our app, Discover is the silver bullet."); GOOG-3047MDL-04918852 at Slide 12 (referring to "recommendations" as "tricks to encourage binge-watching," and stating that "[e]xcessive video watching is related to addiction"); Jin Ex. 38 (("Problematic use" occurs when people feel a lack of control over how they use technology, and this leads to negative life impact (e.g. sleep, parenting, social relationships, or productivity).

[85] *See, e.g.*, META3047MDL-020- 00340672 at 680, META3047MDL-020-00342155.

[86] GOOG-3047MDL-01287601.

[87] Bailliencourt Dep. at 244-247; Kirchhoff Dep. at 331-349.

[88] Bejar Dep. at 217:12-222:24, 402:15-406:8; GOOG-3047MDL-01287601.

[89] Troxel Dep. at 74:2-25.

[90] *Id.*

[91] "Instagram's Newest Test Mixes 'Suggested Posts' into the Feed to Keep You Scrolling" (Jun 23, 2021), https://techcrunch.com/2021/06/23/instagram-suggested-posts-test-topics/.

automatically after 30 days. There is no reason for this limitation other than to revert users to the highly addictive algorithm.

83. Meta also introduced a "separate view from Feed" on March 23, 2022, which "allows users the option to view the latest posts, in chronological order, from up to 50 accounts of their choosing."[92] Notably, Meta only launched this feature five years after first testing it.[93] And this "separate view" does not alter, let alone replace, the main, algorithmically-tailored feed. When asked for the percentage rate of use, Meta represented it "does not maintain data for use or adoption of Favorites in the ordinary course of business."[94] Early testing indicates that the feature received a "low adoption rate."[95]

5. Ephemeral Settings ("Stories" and "Snaps")

84. One hallmark of Instagram, TikTok and Snapchat is the option to make a post or message "ephemeral" – that is, they disappear after a short time (*e.g.*, 24 hours for an Instagram, Snapchat or TikTok "Story"). It is well-known among digital platform designers that ephemeral settings like these drive a phenomenon commonly called **FOMO – Fear of Missing Out**. Knowing that a funny video or a party photo will vanish by tomorrow compels teens to open the app frequently, so they don't "miss" what their friends are doing. It creates a *24/7 urgency* to be online, checking in on the latest Stories.[96]

85. Defendants could have, and should have, eliminated or modified these features for children's accounts. Defendants could have, for example, allowed messages and posts that utilize this feature to remain accessible in an archive for an extended period (*e.g.*, a week) for teen accounts so that teens did not feel pressure to be constantly online. Another approach could be limiting the number of times a minor can view others' stories, to discourage compulsive checking. The platforms did not adopt such limits.

---

[92] *Id.*

[93] ANSWERLAB_00029730 (research summary for Favorites dated July 17, 2017).

[94] Meta's Seventh Supp. Resp. to Interrogatory 12.

[95] ANSWERLAB_00035169.

[96] META3047MDL-136-00013164 at 213 ("Among teens with self-reported low control over their IG usage: [redacted] are concerned about offending friends if they don't respond to their posts or stories right away."); META3047MDL-020-00005380 at 387 ("Triggers of Problematic Use on Facebook… Time-bound (eg, Stories, birthdays) – Catch it before its gone."); SNAP1342034 at 045 ("The ephemeral nature of Stories requires users to develop a daily habit of checking them.").

6. Notifications

86. An additional method that each of the Defendants utilize to increase use of their platforms is strategically timed notifications. Notifications present a message intended to encourage a user that is not on the platform to come back, and may cause the user's phone to vibrate or ring. The Defendants carefully time these notifications to maximize the amount of time that users spend on the platform.[97]

87. These notifications – another form of dark pattern – can be highly effective at influencing behavior, particularly for kids. TikTok documents, for example, describe its notification system as one of "many **coercive design tactics that detract from user agency**," *i.e.*, "the capacity of individuals to act independently and to make their own free choices" [98] It goes on to acknowledge that "**user agency is very limited on TikTok due to the problems we see related to addictive behavior**."[99] TikTok acknowledged that its notification strategy was growing the platform "at the expense of their users," and benefiting "companies and advertisers more than users."[100]

88. Meta similarly describes its "low-value notifications" as part of its platforms' "'addictive'-like design" and "dark pattern."[101] Surveys conducted by Meta on teen users found that that "[redacted] of US teen WAU [weekly active users] say notifications make it harder for them to manage the amount of time they spend on the app, and [redacted] say **the number of notifications they receive can**

[97] *See, e.g.*, Kirchhoff Dep. at 271:10 - 275:5, 281:11 - 284:1 (discussing TikTok's notification strategy); TIKTOK3047MDL-002-00101297 (discussing need to "Find the best push time and the best push count for every user to maximize dau and retention."); TIKTOK3047MDL-004-00321758 at -799 ("By optimizing the grouping arrangement of off-app push on Android in the message center, the exposure of out-of-app messages can be improved, and the overall click through rate of out-of-app messages can be improved."); SNAP1257256 at -262, -263 ("experimenting" with sending notifications at a user's "predicted 'best hour'" for increasing use); GOOG-3047MDL-01062790 (targeting notifications "based on knowledge of interests, viewing habits, time-of-day, etc." as part of its "two-pronged approach to growth"); META3047MDL-019-00015192 at -193 ("Optimizing the time of day that we send push notifications . . . ."); META3047MDL-047-00990649 at -666 ("This launch post Growth Notifications team shows that adding time-of-day increase engagement by better optimizing SmartScheduler. . . ."); META3047MDL-034-00123032 at -035 ("Time of day churn Notifications have higher CTR which drives increase in weekly active users"); META3047MDL-047-00242378 ("Researching the best time of day to send push campaigns reveals that noon" and "8-9pm are ideal times.").

[98] Furlong Dep. at 82:23 – 86:11 (emphasis added); Furlong Ex. 5.

[99] *Id*.

[100] TIKTOK3047MDL-006-00327425 at -444.

[101] META3047MDL-044-00108564 at -566.

be overwhelming."[102] Many teens "reported that notifications lead them to use FB [Facebook] more often than they want."[103]

89. YouTube documents describe notifications as part of the platform's "behavior science" efforts to get users "hooked."[104] In fact, YouTube sends 2.5 billion notifications per day, including both "contractual notifications" to subscribers and "affinity notifications" to non-subscribers.[105]

90. Snap similarly uses push notifications to drive user engagement.[106] In June 2019, Snap had 203 million active users and sent 11 billion iOS notifications per day.[107] Snap sends notifications for a variety of purposes such as receiving a new chat or photo message, a friend posting to their story, Snap suggesting a new friend, new subscription content becoming available, and location-based notifications.[108]

91. The Defendants could have, and should have, greatly limited notifications on teen accounts. The Defendants could have, and should have, silenced notifications during hours that teens should be in school or sleeping. They also could have, and should have, limited notifications on teen accounts to events that may require a direct action by the teen, such as a direct message from a friend. "Low-value" notifications that serve no purpose other than to drag users back to the platforms (*e.g.*, notifying users that someone they don't follow has posted something[109]) should not have been sent to teen accounts.

92. In 2023, after years of complaints that notifications were interfering with children's sleep, Meta introduced a "Quiet Mode" feature, which turned off notifications at night for minor accounts, so that they would not "feel compelled to be looking at their phone" during hours when they should be sleeping.[110] However, this feature was implemented as an "opt-in" feature, ensuring

---

[102] META3047MDL-136-00013164 at -213 (emphasis added).

[103] META3047MDL-044-00171345 at -360.

[104] GOOG-3047MDL-02009802; *see also* GOOG-3047MDL-04625648 at 6 (in analyzing "Google Products & Tech Addiction," YouTube notes an overlap between "Fear of Missing Out" and "Push notifications).

[105] GOOG-3047MDL-02113187.

[106] SNAP0886473; SNAP5147058; Tran Dep. at 89:17-90:16.

[107] SNAP0098654.

[108] Tran Dep. at 40:9-46:2; Tran Dep. at 104:17-25.

[109] *See, e.g.*, https://www.reddit.com/r/Instagram/comments/q6ijfq/how_to_turn_off_notification_account_3_others/ (Instagram users complaining about irrelevant notifications like these and the difficulty of turning them off).

[110] Bejar Dep. at 583:17-584:1.

it would not be widely used.[111] As one Meta engineer explained, "[s]ecurity features that were opt in, no matter how much protection they're afforded, . . . had extremely low adoption rates."[112] Thus, the only impact of a feature like this "would be in a press release because it wouldn't effectively be preventing teenagers from getting notifications at night."[113] (Meta also allows users to select what types of notifications they receive, but this option was buried in a settings menu and difficult to understand and use.[114])

93. It similarly took TikTok until October 2021 to finally roll out nighttime restrictions on push notifications to users younger than 18 in the United States.[115] The new policy they put in place as a default setting restricts push notifications from 9 p.m. to 8 a.m. for 13- to 15-year-old users, and from 10 p.m. to 8 a.m. for 16- to 17-year old users.[116] Neither Meta nor TikTok has announced any initiative to limit notifications to teens during school-time hours.

94. YouTube announced in 2018 that users could have more control over when they received notifications by "bundl[ing] all of your YouTube push notifications into a single notification each day and set a specific time to receive your digest."[117] However, as with the notification options discussed above, this feature was not enabled by default, and was hidden in a setting menu.

95. Snap implemented similar notification restrictions based on time-of-day as an "annoyance mitigation" strategy.[118] However, in November 2023, Snap's Growth Team sought to shrink quiet hours from 12-7am to 3-6am, forecasting a 650,000 increase in daily active users.[119] Snap considered removing quiet hours altogether by continuing to send notifications at all hours of the

---

[111] Bejar Dep. at 584:2-6.

[112] Bejar Dep. at 545:12-16; *see also* Bejar Dep. at 547:16-22 ("teenagers . . . don't go into settings"). This is borne out by the data: only 4.6 million accounts (out of hundreds of millions of teen accounts) used the tool in 2020. META3047MDL-003-00181350 at -360. *See also* Meta's Sixth Supp. Resp. to Interrogatory 12 (identifying the following adoption rates, among others: Ad Topic Controls [redacted], Limit Interactions [redacted], Pinned Comments [redacted], Family Center Supervision [redacted]); Meta's Seventh Supp. Resp. to Interrogatory 12 (Take a Break [redacted]).

[113] Bejar Dep. at 584:9-12.

[114] *See, e.g.*, https://www.reddit.com/r/Instagram/comments/q6ijfq/how_to_turn_off_notification_account_3_others/?rdt=58028 (Instagram users complaining about irrelevant notifications like these and the difficulty of turning them off).

[115] TIKTOK3047MDL-002-00101838.

[116] *Id.* at -841.

[117] GOOG-3047MDL-00000058 at -060.

[118] SNAP1974307: SNAP2058230; SNAP6014524.

[119] Tran Dep. Ex. 3.

day but doing so without sound between 12am and 7am.[120] Snap has never implemented any push notification policies that are tied or connected to user age.[121]

7. Appearance-Altering Filters

96. Snapchat,[122] TikTok,[123] Instagram,[124] and YouTube "Shorts"[125] all provide (or provided) filters or effects that change how a user's photo or video looks. Filters may, for example, slim the face, smooth skin, enlarge eyes, add makeup, or make other "beautification" enhancements. As the defendants acknowledge in documents, the use of these filters is popular with teens, and can fuel body dysmorphia, low self-esteem, and unhealthy beauty standards, particularly among teen girls.[126] Frequently, these harmful effects are described, both in public and in internal company documents, as "Snapchat Dysmorphia."[127] Given these known harms, the Defendants could have, and should have, **eliminated appearance-distorting filters for minors**.

97. TikTok has acknowledged that it is "behind the industry" in addressing the known harms of beauty filters,[128] and that its safety team has long opposed beauty filters but did not get traction

---

[120] SNAP2986191.

[121] Tran Dep. at 110:6-15.

[122] SNAP2812798.

[123] TIKTOK3047MDL-004-00141896.

[124] [redacted] Ex. 18 at 2 - META3047MDL-050-00003832 at -833.

[125] GOOG-3047MDL-00442481; GOOG-3047MDL-01786683; GOOG-3047MDL-03133836; Dep. of Google/YouTube (C. Niedermeyer), April 16, 2025, at 73:4-75:17.

[126] *See, e.g.*, SNAP2926182 at -182 ("viral lenses have also proven to be a great tool to drive incremental growth"); META3047MDL-020-00609932 at -941 ("The altering of selfies appears to be connected with negative impacts on both the person posting it, and those viewing it in terms of **mental health, body dissatisfaction, and eating disorder behaviors**.") (emphasis added); META3047MDL-037-00007066 ("[T]here is substantial evidence to suggest that Instagram and Facebook use can increase body dissatisfaction."); META3047MDL-037-00007066 (discussing how Instagram can contribute to "downward spirals" and create a "perfect storm" of harms, leading to eating disorders, body dysmorphia, body dissatisfaction, depression and loneliness); META3047MDL-040-00337135 at -135, -136 ("These extreme beauty effects can have severe impacts on the individual using the effects and those viewing the images"); Furlong Ex. 18.; Dep. of Google/YouTube (C. Niedermeyer), April 16, 2025, at 74:15-75:17; GOOG-3047MDL-01773257 (produced in Native) at Slide 57; GOOG-3047MDL-03133836; GOOG-3047MDL-03524164 at -167.

[127] Brody Dep. at 187:7-188:23 ; SNAP0078233 at -243; SNAP0525938; SNAP0933724; SNAP0525939; Furlong Dep. at 127:11-139:21.

[128] Furlong Dep. at 121:4-19, 150:14-153:5.

due to concerns about negatively impacting user growth metrics.[129] TikTok finally announced restrictions on appearance filters for under-18 accounts at the end of 2024.[130] Meta likewise eliminated beauty filters in 2025, more than eight years after they were first introduced.[131] Appearance altering filters are still available on Snapchat and YouTube Shorts.

8. Location Sharing (Snap Map)

98. Snapchat's "Snap Map" feature (launched 2017) allows users to see their friends' real-time locations on a map. This feature raises serious privacy and safety concerns for young users. A teenager broadcasting their location can inadvertently reveal sensitive information – like their home address, the school they attend, or their whereabouts at a given moment – to all their Snapchat "friends," who might include acquaintances or even people they have never met in person.

99. Snap Map can also significantly intensify FOMO (fear of missing out) by showing users where their friends are and what they are doing in real time.[132] Seeing others at parties, events, or social gatherings can lead to feelings of exclusion and loneliness – particularly for teens and young adults.[133]

100. In 2019, Scottsdale, Arizona, witnessed the arrest of 34-year-old Steven Anthony Spoon in connection with a series of "Peeping Tom" incidents targeting teenage girls. Spoon's method, as detailed in court paperwork and police statements, involved a calculated use of Snapchat's features. He told investigators that he would create fake Snapchat profiles, posing as a teenage girl to befriend other underage girls on the platform. Crucially, he then exploited Snap Map by identifying victims who had their location settings enabled, allowing him to pinpoint their homes.[134] Spoon is alleged to have targeted at least 11 houses over a period of months, spying on teenage girls through their windows as they were changing or showering.[135]

---

[129] *Id.* at 150:14-153:10; 159:6-162:8, 164:21-165:8, 188:18-190:9, 214:16-24.

[130] Furlong Dep. at 125-26, 135, 145, 157, 175-77, 187, 194-95.

[131] "Meta is Ending Support for Custom Face Filters in Its Apps" , The Verge, (August 27, 2024) https://www.theverge.com/2024/8/27/24229643/meta-spark-ar-effects-face-filters-shutdown-tiktok-snapchat.

[132] SNAP7347297; SNAP0031913.

[133] SNAP0939251; Beauchere Dep. Ex. 48; SNAP0231603.

[134] "Parkours with a Motive: Police say Peeping Tom Jumped Over Fences to Look at Teen Girls He Met on Snapchat", ABC News (October, 2019) https://www.12news.com/article/news/crime/scottsdale-peeping-tom/75-27e3e2c5-09be-4a68-a411-af23993e26cc.

[135] *Id.*

101. In another disturbing case from 2023-2024, 20-year-old Victor Ferman allegedly utilized Snapchat's location-sharing capabilities to stalk a 15-year-old girl in the League City and Pearland areas of Texas. According to police statements, Ferman discovered the victim's home address because her live location-sharing feature on Snapchat was activated. The victim and Ferman had reportedly never met in person; their interaction began on social media, initiated through a mutual acquaintance. [136]

102. Snap could have, and should have, eliminated or at least restricted this feature for minors. Short of turning it off altogether, Snap could have, for example, restricted minors' ability to share precise locations, allowing them to show only their general city or neighborhood, rather than an exact pinpoint. It could also have made location sharing time limited, such that it turned off automatically for minors after a short period, requiring re-confirmation to turn it back on. Snap, instead, continues to allow teen users to share their precise location for extended periods.

* * *

103. Each of the above design elements contributed to making the platforms more "sticky" – encouraging longer sessions, more frequent use, and deeper psychological attachment. But they also each had the effect (often clearly foreseen) of increasing risks to young users' mental and physical health, sleep, privacy, or safety. Importantly, none of these features were essential to providing a social networking service; they were enhancements adopted to drive engagement metrics. Removing or modifying them would not have broken the apps – it would have just made the apps less addictive. Where such conflicts arose, the Defendants all too frequently chose addiction and profit over safety.

104. Notably, the Defendants never warned children, parents/guardians or the public that their platforms were designed to addict.[137] Instead, they have attempted to obscure the issue. For example, Meta employees were instructed not to use the word "addiction"; instead "you were supposed to say 'problematic use.'"[138] The topic of addiction was considered "radioactive," and employees were discouraged from researching or even talking about the issue.[139]

---

[136] "The Surging Dangers of Location Sharing: Snapchat Stalker" (February 26, 2024), https://www.bryanfagan.com/blog/2024/02/the-surging-dangers-of-location-sharing-snapchat-stalker/.

[137] *See, e.g.*, Bejar Dep. at 144:6-15, 436:16-22 (Meta did not "warn the public, kids, or parents" about "the increased risk to kids of addiction or problematic use from Instagram"); Han Dep. at 176:17-177:6.

[138] Bejar Dep. at 136:6-137:20. Executives occasionally revealed the company's equivalent treatment of those words. For instance, Adam Mosseri, the Head of Instagram, told a podcast interviewer that it was "reasonable" to equate "addiction" to social media with the company phrase "problematic use." Mosseri Dep. Exhibit 6 (clip from "Byers Market" podcast).

[139] Bejar Dep. at 137:14-25.

B. Defendants Could Have, and Should Have, Implemented Stronger Default Privacy Settings

105. The Defendants' platforms were not reasonably safe for children for the additional reason that they lacked proper default privacy settings for minors, creating an unnecessary and unreasonable risk of harm to children from bullying, harassment, and sexual predation by strangers. Public accounts and lack of default privacy settings increase the risk that minors will be harassed by strangers and targeted by sexual predators. There is a stark difference between a platform that is "open by default" versus one that is "private by default" for a teenager. In an "open by default" environment, where (for example) strangers can find a child's account and message them directly or comment on their posts, children are frequently the target of unwanted sexual advances and harassment from strangers, as well as efforts at grooming, sextortion and sexual assault. These risks and behaviors are well-known among digital platform designers,[140] and child-safety experts have urged strong default privacy for minors as a basic safeguard for more than a decade.[141]

106. In spite of these known risks, for years, the Defendants took the "open by default" approach, and treated teen accounts essentially like adult accounts, visible to a wide audience unless the user changed settings, and open to contact from strangers unless the teen proactively navigated into the settings menus to turn privacy settings on. The Defendants implemented these "opt-in" privacy settings even though it is widely understood among digital platform designers that opt-in features (in contrast to defaults) are far less likely to be used. Data from Meta, for example, shows that only 9% of teens change a privacy setting at all.[142] In fact many safety features touted by the company have [redacted] adoption rate.[143] Teens are also less likely than adults to actively engage with safety tools, underscoring the importance of defaults for teen accounts.[144] As one former Meta safety engineer testified, "teenagers . . . don't go into settings,"[145] and, in most

[140] *See, e.g.*, META3047MDL-047-00346088; TIKTOK3047MDL-014-00330672 at 81; Brody Dep. Ex. 17.

[141] META3047MDL-031-00136977 at 995.

[142] META3047MDL-031-00024886.

[143] *See* Meta's 6th and 7th Supp. Resp. to Plts. Second Set of Interrogatories, at No. 12. (showing adoption rates for various features).

[144] *Id.*

[145] Bejar Dep. at 548:16-22; *see also id*. at 582:3-10 (Q. "What impact would those features of parental supervision have for adoption and effectiveness based on your industry experience?" A. "It would mean that the feature would not be adopted and then as such would not be effective as a safety feature.").

cases, "[i]f a feature is opt-in, almost nobody will use it."[146] Or as a TikTok executive put it, "**anything opt in gets very low usage**."[147]

107. Examples of stronger default privacy settings that were available include:

1. Private Accounts by Default

108. For most of the last decade, if a 13-year-old signed up for Instagram or TikTok, the **default setting made their new account public**, meaning anyone can find and follow them and see their posts. The teen had the *option* to go into settings and make their account private, but that relied on awareness of the feature, as well as a deliberate choice and exertion of effort to turn it on. This likely was better for engagement – public content will generate more interactions than private content – but not for teen safety.

109. Defendants could have, and should have, made all accounts for users under 18 **private by default**, only visible to people they approve as followers. This way a teen would have to opt *into* being public, an action that would at least be deliberate and not accidental.

110. It was not until 2021 – more than 10 years after Instagram's founding – that it announced new accounts for kids under the age of 16 would default to private. Despite this announcement, existing teen accounts were not switched to private. Moreover, the private default was a pre-clicked bubble in the set up menu that could be instantly changed to public in the same screen, and thus not a strong default.[148] (Most default settings must be changed by navigating through settings menus, which teens are much less likely to do.) TikTok likewise waited until 2021 to default accounts of users under 16 to private.[149] In both cases, these changes appear to have been made in response to regulatory action (new UK laws, for example, required children to be defaulted into the highest privacy setting).[150]

---

[146] Bejar Dep. at 167:15-24 (emphasis added).

[147] TIKTOK3047MDL-098-04111887 at -898.

[148] Jayakumar Dep. at 71-73.

[149] Siladitya Ray, TikTok Accounts of Younger Teens Will Now Be Private By Default, All Minor Users Will Have Tighter Privacy, Forbes (January 12, 2021) https://www.forbes.com/sites/siladityaray/2021/01/13/tiktok-accounts-of-younger-teens-will-now-be-private-by-default-all-minor-users-will-have-tighter-privacy/.

[150] "Age Appropriate Design: A Code of Practice for Online Services, Information Commissioner's Office," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/7-default-settings/.

2. Stricter Contact and Messaging Settings

111. A related issue is how easy it is for **unknown adults or strangers to contact minors** on these platforms. Historically, default settings on Facebook, Instagram and TikTok allowed anyone to send a friend request, follow, or direct message a teen user, and to comment on a teen user's post.[151] Similarly, on YouTube, anyone was able to comment on a teen user's video and could likewise direct message a teen user. Perhaps most insidiously, the Defendants' recommendation algorithms also recommend content created by teen accounts to adults, meaning that adult strangers would see videos and pictures posted by teens in their feeds.[152] Making matters worse, because the recommendation algorithms seek to encourage engagement, adults who show a particular interest in pictures and videos posted by young teens were more likely to get more of them in their feed.

112. Internal Meta documents highlight the problem. They note that "there is no current mitigation [] in the Reels product roadmap" for "predatory DMs from adults sent to minors who are more easily discovered via their Reels content."[153] As Meta engineers acknowledged, "bad actors can signal one another and look for and connect with kids and then enter a private messaging thread," creating "one seamless flow of discovery-->connection--->harm."[154]

113. The net result is that children frequently receive unwanted sexual messages from strangers on these platforms.[155] For example, as noted above, a survey conducted by Meta found that 13% of children aged 13 to 15 on Instagram reported unwanted sexual advances in just the last seven days.[156] Similarly, 4 in 10 TikTok users reported encountering inappropriate content related to minor safety in user-to-user interactions.[157] In 2022, Snap was informed by multiple law enforcement agencies that over 80% of the child sexual grooming cases handled by the agencies

---

[151] "Strengthening privacy and safety for youth on TikTok," TikTok, (Jan. 13, 2021), https://newsroom.tiktok.com/en-us/strengthening-privacy-and-safety-for-youth; TIKTOK3047MDL-079-LARK-02426130.

[152] *See, e.g.*, META3047MDL-020-00271442 ("Our existing classifiers do not work great on short form virality that there is no current mitigation for in the Reels product roadmap – namely, predatory DMs from adults sent to minors who are more easily discovered via their Reels content."); META3047MDL-014-00369785 at 86 (discussing how "bad actors can signal one another and look for and connect with kids and then enter a private messaging thread," creating "one seamless flow of discovery-->connection--->harm.").

[153] META3047MDL-020-00271442.

[154] META3047MDL-014-00369785 at 86.

[155] *See, e.g.*, META3047MDL-014-00046829 ("girl teens being 32x more likely to get unsolicited sex talk on IG compared to FB"); Baldwin Dep. Ex. 11.

[156] META3047MDL-004-00015029 at -033, -049.

[157] TIKTOK3047MDL-002-00102517, -527.

are associated with Snapchat.[158] An internal YouTube presentation shows that 8% of minors reported having a sexual interaction on YouTube, and acknowledges that "predators can begin extorting minors through relationship building on YouTube before moving the conversation off platform."[159]

114. The Defendants could have, and should have, created default settings that limit all inbound communications for minors – including DMs and comments – to only people they know (*i.e.*, contacts they have explicitly approved). The Defendants also could have, and should have, prohibited adult accounts from sending friend requests to minor accounts, requiring contact to be initiated by the minor. Moreover, the same credit card age verification technology discussed in Opinion 2 below, which the platforms failed to provide, could have marked all known adults and stopped them from pretending to be kids if they had previously signed up as adults. Facial recognition technology, also discussed in Opinion 2 below, would have been even more powerful, as the platforms could accurately estimate each user's age within a few years, further preventing adults from pretending to be teens. All of these things were possible with thoughtful design but were not done.

115. In 2021 – more than 10 years after its creation – Instagram for the first time introduced several new features purporting to reduce inappropriate interactions between children and adults. However, these tools had significant gaps:

- **Restricted DMs (released March 2021):** This feature purported to restrict adults over 18 from starting private chats with teens they're not connected to. It also uses prompts to encourage teens to be cautious in conversations with adults they're connected to.[160] However, as discussed in more detail in Opinion 2 below, Instagram does not perform any meaningful verification of a user's age, relying instead on the age given by the user during sign-up. As a result, an adult wishing to avoid this restriction can simply lie about their age and create an account that appears to belong to a child.[161] Moreover, a majority of teens are signed up on the platforms using adults' birthdays, meaning their accounts are not protected by this feature.[162] Perhaps not surprisingly, Meta employees observed a year after the feature launch that "there have been many gaps in fulfilling our promise" to "block teens from receiving DM requests from non-teens."[163] Indeed, internal documents indicate that teens were continuing to receive "unwanted DM requests" from "senders with stated age 18-20," "senders with no stated age," and "senders outside the US who state they are

[158] Baldwin Dep. Ex. 11.

[159] GOOG-3047MDL-02432112 at 20.

[160] Our Tools, Features, and Resources to Help Support Teens and Parents, Meta https://www.meta.com/help/policies/809291991003600/.

[161] *See* META3047MDL-003-00014331.

[162] Jayakumar Ex. 71 at 16 ("60% of actual teens lie and say they're non-teens").

[163] *Id.* at 15-16.

teens, but may not be teens."[164] I have seen no evidence that Meta disclosed these risks to the public, despite these same documents acknowledging that "most DM requests are unwanted," "unwanted DM requests are integrity and acquisition risks for teens," and "DMs are the most problematic interaction vector for teenagers on Instagram, including bullying, harassment, and more severe violations."[165]

- **Restricting teen account discovery (released July 2021):** Prior to July of 2021, accounts that showed an interest in content posted by young children, including sexually suggestive content, were recommended more of that content by Instagram's algorithms. In other words, Instagram actively connected potentially predatory adults with young teen accounts.[166] In 2021, Instagram launched this feature to identify accounts of "suspicious" adults and stop recommending underage content to those suspicious accounts. But again, adults could avoid this restriction by lying about their age in order to create what appeared to be a child's account.[167]

- **Default Private Accounts for Users Under 16 (released July 2021):** As noted above, this feature made new accounts of users under the age of 16 private by default. However, it did not apply retroactively to under-16 accounts that had already been created, and it could be turned off by teens without permission from parents.

- **Restricted tags and mentions (released December 2021):** This default setting restricts people from tagging or mentioning teens that don't follow them.

116. Given the gaps in these features, it is perhaps not surprising that they were not particularly effective at preventing unwanted contact between adults and teens. As just noted, a 2019 survey of Instagram users taken before the features were implemented found that 13% of children aged 13 to 15 had experienced unwanted sexual advances on the platform in the last seven days.[168] These unwanted contacts came overwhelmingly from people that the child did not know.[169] After the introduction of the first three restrictions referenced above, another survey was conducted.[170] The numbers were essentially unchanged: 13% of children aged 13 to 15 reported unwanted sexual advances in the past seven days.[171]

[164] *Id.* at 15.

[165] *Id.* at 9-10.

[166] *See* Sinha Ex. 8.

[167] *See* META3047MDL-003-00014331.

[168] Bejar Dep. at 307:10-17.

[169] Bejar Dep. at 319:8-23.

[170] The BEEF survey was conducted from July to September of 2021. Bejar Dep. at 365:5-16.

[171] Bejar Dep. at 341:24-342:10.

117. The other Defendants likewise waited unreasonably long to put in place restrictions on communications with teens. TikTok did not disable direct messaging by adults to users under 16 until 2020;[172] and Snapchat did not restrict friend suggestions and requests for kids until 2022.[173] YouTube discontinued direct messaging altogether in 2019, though it continues to allow all users to comment on videos by default, including those posted by teens.

118. Notably, TikTok introduced other features, over the objection of its safety team, that encouraged inappropriate contact between minors and adults. For example, in 2019, TikTok began allowing users to send other users what essentially operated as cash "gifts" during TikTok LIVE livestream videos. By 2022, Forbes was reporting that TikTok LIVE had become "A Strip Club Filled With 15-Year-Olds'," detailing how viewers used TikTok LIVE comments to urge young girls to perform sexual acts in exchange for gifts and off-platform payments and highlighting the risks of sexual exploitation and abuse for underage users on the platform.[174]

119. Members of TikTok's safety team testified that they had warned TikTok's management about this issue but got no traction, as management did not believe the harms were "severe enough."[175] TikTok documents note that this type of "transactional" sexual content on TikTok Live was increasing key business metrics like revenue, watch time, and user engagement, creating a conflict between safety and commercial success.[176] At one point TikTok reported there were 112,000 livestream hosts under 14 years old on the platform and 1 million "gifts" being exchanged for adult content every month.[177] While only accounts with a recorded age above 16 were permitted to livestream on TikTok, as explained in more detail below, due to lack of age verification, children under 16 who lied about their age would still have access to this and other supposedly blocked

[172] "TikTok to Launch Parental Controls Globally, Disable Direct Messaging for Users Under 16," TechCrunch, (April 16, 2020) https://techcrunch.com/2020/04/16/tiktok-to-launch-parental-controls-globally-disable-direct-messaging-for-users-under-16/.

[173] Prior to 2023, Snapchat's "Quick Add" feature (suggesting people you may know) enabled strangers to pop up as suggestions to teens, and for teens to pop up as suggestions on strangers' accounts. In 2023, after some high-profile tragedies (including drug dealers contacting teens), Snapchat announced it would limit the friend suggestions for teen users so that they would only see suggestions of people who have a certain number of mutual friends in common. This was to reduce the chance of strangers (with no or few mutual connections) appearing in teen feeds. "Snapchat Adds New Safety Fetures for Teen Users" (Sep 7, 2023), https://www.cbsnews.com/miami/news/snapchat-adds-new-safety-features-teen-users/.

[174] Maher Dep. at 78:2–78:6, 81:10–82:4, 116:3–116:7, 124:5–124:10, 146:21–146:25, 166:20–167:9; Maher Dep. Ex. 9.

[175] Maher Dep. at 151:3-152:12, 161:13-161:18, 166:17-167:20; Maher Dep. Ex. 16.

[176] Han Dep. at 372:20-376:6, 379:12-380:22, 381:2-381:15; Han Dep. Ex. 50.

[177] Han Dep. at 376-19-377:10, 409:7-414:15; Han Dep. Ex. 51.

features.[178] Additionally, 16- and 17-year old users were provided full access to this feature that, through its design, was known to encourage transactional sexual content.

3. Data Minimization for Youth Profiles

120. While not as visibly apparent to users, another important design choice by the Defendants was how much data to collect from and about minors, and how to deploy that data. Defendants generally treated minors almost the same as adults in terms of data harvesting – tracking their activity, preferences, locations, and using that data for ad targeting and algorithmic tuning.[179]

121. A safer approach for children's accounts (and one advocated by privacy regulators) is **data minimization**: collect the least amount of personal data necessary for the service, especially when the user is a child. For instance, there is rarely a need to track a 14-year-old's precise ad clicks or watch history in perpetuity.

122. Platforms designed their data pipelines to vacuum up everything for all users by default. They could have, and should have, introduced different data collection settings for teens, where much data is either not collected or automatically deleted after short periods. Doing so might slightly reduce advertising efficiency or personalization – a trade-off favoring well-being over maximum monetization.

123. The Defendants did not initially design their systems to minimize teen data. To the contrary, internal records from Facebook show that monetizing teens (and even younger children's data) was considered a growth vector.[180] Only after regulations like the European GDPR and the UK Age Appropriate Design Code came into play did companies start to pare back some data practices for minors.

124. For example, in 2021 Google announced that YouTube would stop serving personalized ads to anyone under 18 (a step toward data minimization, since it doesn't need to track as much behavior for targeting) and that location history would be off for accounts of minors.[181] Facebook likewise announced it would restrict targeting of ads to minors to a few categories (age, gender,

[178] Maher Dep. at 75:6–75:20, 76:12–77:1; Maher Dep. Ex. 7.

[179] SNAP7301586; SNAP7301586.

[180] META3047MDL-207-00022339 at 43.

[181] "Google to Introduce Increased Protections for Minors on its Platform, Including Search, Youtube and More," TechCrunch, (August 10, 2021) https://techcrunch.com/2021/08/10/google-to-introduce-increased-protections-for-minors-on-its-platform-including-search-youtube-and-more/.

location) rather than a full behavioral profile.[182] Similarly, TikTok announced on July 3, 2024 that advertisers would no longer "be able to reach teens in the United States using any personalized targeting and campaign selections."[183] In 2023, Snap restricted ad targeting for users under the age of 18, but only applied the policy to users in the EU.[184] In 2023, TikTok announced that it would no longer serve personalized ads for accounts aged 13 to 15.[185] These changes illustrate feasible dial-backs in data collection that could have been implemented much earlier.

125. Instagram introduced a Teen Accounts feature in September of 2024; however, they continue to collect expansive data on teen accounts.[186]

126. In short, designing for privacy was possible, but it usually ran counter to the profit motive. Defendants chose not to flip those switches until legal compulsion loomed. The consequence was that, for many years, teens were subject to intense data surveillance and profiling, which increased their exposure to manipulative advertising and potentially even security risks (in the event of data leaks). A safer design philosophy from the start would have been "we don't keep what we don't need" when it comes to kids' data.

The Defendants, moreover, could have, and should have, alerted kids and parents to these data collection practices, so that kids and parents could make an informed decision about whether to use the platform. To the extent the defendants disclosed this at all, the disclosure was typically buried in massive "terms of service" that the Defendants knew users were extremely unlikely to read.

* * *

127. In all three of these areas – account visibility, communications and data collection – the theme is the same. The **default settings** for young users could have been set to **maximally safe/private**, but instead were set at more open, risky levels that align with growth and engagement strategies. Changing a default is one of the simplest design changes there is; it often involves no

[182] "Instagram to Default Young Teens to Private Accounts, Restrict Ads and Unwanted Adult Contact," TechCrunch, (July 27, 2021) https://techcrunch.com/2021/07/27/instagram-to-default-young-teens-to-private-accounts-restrict-ads-and-unwanted-adult-contact/.

[183] "Enhancing Privacy and Control: New Ad Experience and Tools For TikTok Users and Advertisers," TikTok for Business, (July 3, 2024) https://ads.tiktok.com/business/en-US/blog/enhancing-privacy-control-advertisers-users.

[184] SNAP7301586.

[185] "Updates to Ads for Teens and Improved Sata Control and Transparency Tools, TikTok for Business" (June 28, 2023) https://ads.tiktok.com/business/en-US/blog/privacy-updates-improved-data-control-transparency-tools?acq_banner_version=73412989.

[186] "Are Instagram Accounts Really Protected- Even From Meta?," Tuta, (April 17, 2025) https://tuta.com/blog/instagram-teen-account-data-collection.

more than a few lines of code or a settings configuration. The fact that changes only occurred after significant delay, or not at all, indicates these companies were not prioritizing children's privacy in their design decisions.

C. Defendants Could Have, and Should Have, Implemented Features That Limit the Platforms' Harms

128. Given the known negative effects of their platforms on children, Defendants could have (and should have) implemented features designed to limit these harms and promote healthier usage and well-being. There was no shortage of ideas in this category – academics, child development experts, and the Defendants' own employees have recommended numerous features to help users, especially teens, have a more balanced experience on these platforms.

129. The Defendants, however, failed to promptly implement effective safety features. Each of the Defendants has, over the years, implemented features that ***purport*** to make their platforms safer for children. These features, however, typically came many years after the platforms were created, after millions of young children had already gained access and spent significant time on them. They were therefore too late to prevent significant harms to millions of children. Additionally, even when safety features were implemented, in many instances they were designed in ways that were known to be ineffective.

130. As explained in more detail below, the core cause of these failed safety efforts is the Defendants' prioritization of growth over safety – something that was built into the tracking systems they put in place. While the Defendants carefully tracked growth and engagement metrics and used those metrics in evaluating design changes, they largely ignored metrics related to the wellbeing of their users. The result was that engineers had to ensure that new "safety" features would not reduce engagement and time spent on the platforms – even though less time on the platforms was exactly what many kids need.

131. Below I discuss how such tracking systems could (and should) have been used to protect the wellbeing of children, and how the Defendants' tracking systems had the opposite effect. I then discuss some key positive design opportunities that were feasible but largely ignored during the critical years:

1. Systems to Identify, Track and Limit Harms

132. At the core of every digital platform is a system of metrics. The company selects metrics to track, sets goals for those metrics, then evaluates the performance of its engineers – and the features and initiatives they create – based on those metrics and goals. The decision of which metrics to track and what goals to set define how the platform will operate and how it will change over time. Whether a company acknowledges it or not, those metrics define the company's values.

133. For AngelQ, we have set up the platform to track numerous metrics related to the wellbeing of our users, and set goals based on those metrics. For example, we track the time that children spend on our platform and ensure that screentime does not cross over into unhealthy levels of usage. Our features are designed and evaluated based on these types of metrics. Thus, if a new feature unexpectedly causes a large, and unhealthy, jump in screentime, our engineers can see it and quickly correct for it.

134. Defendants could have, and should have, (i) put systems in place that track the harms children experience on their platforms, (ii) set goals for reducing those harms, and (iii) used those goals to evaluate the performance of their engineers and the features they designed. The evidence I have reviewed indicates that they instead focused almost entirely on growth metrics.

135. According to former Meta employees, for example, Meta carefully tracked metrics like "sessions and engagement and growth."[187] Those metrics were then used by managers to evaluate the performance of engineers, and to determine those engineers' compensation. In other words, if you are a Meta engineer, "you're going to get paid more money . . . for driving usage."[188] The reason for this focus on engagement is straightforward: the Defendants "make more money" if their users are on the platform for longer periods of time.[189] (The other Defendants have similar business models and incentives.[190])

136. In contrast, Meta had no "comprehensive metrics framework that incentivized the team to reduce the harms" to children.[191] The team that was nominally assigned to work on safety issues "was not well-resourced enough" and was "tragically small relative to the impact that users were having."[192]

137. Former Meta engineer Arturo Bejar testified that it was this incentive structure and lack of adequate resourcing for safety – not any issues with feasibility – that prevented Meta from implementing "meaningful safety tools and features."[193] That is because implementing effective safety measures "can have a negative impact on users' engagement on the app," and could

[187] Bejar Dep. at 150:5-11.

[188] Bejar Dep. at 153:8-17.

[189] Bejar Dep. at 149:15-23.

[190] *See, e.g.*, Furlong Dep. at 44:23-50:11, 248:5-13 (acknowledging that TikTok's business model encourages optimizing for user time spent on the platform); GOOG-3047MDL-00579554 (launching YouTube's goal to reach 1 billion hours of watch time per day by 2016, which would mean $50 billion); GOOG-3047MDL-02024105 (launching goal to reach 4 billion hours by 2020); SNAP7138431 (Performance Review for Snap's Head of Growth).

[191] Bejar Dep. at 146:1-4.

[192] Bejar Dep. at 147:23-148:5; Jayakumar Dep. at 195:11-196:4.

[193] Bejar Dep. at 157:19-20, 157:11-19.

therefore "decrease the amount of money Meta makes."[194] Meta was "not willing to substantively address the issue of reducing the time that people spend" by, for example, silencing notifications, even though "[r]educing those things might help addiction."[195]

138. A stark example of this is Facebook's reporting systems. The nominal purpose of its reporting system is so that users can report harms that they have experienced on the platform. In principle, this could have allowed Meta to adjust its platform in ways that reduce those harms. In practice, however, Meta's reporting system was broken. Meta chose to add "friction" into the system so that most users who started the reporting process would not complete it. [196] In fact, the system included a feature that led users to "believe they had submitted a report" when, in fact, they had "dismissed" the report.[197] Meta made these design changes "***to discourage reporting***."[198] It should come as no surprise that Meta failed to reduce harms on its platform, when it did not even have a functioning system to track them, much less prioritized internal goals oriented towards reducing them.

139. TikTok documents and testimony point to a similar issue. Documents indicate, for example, that TikTok lacked any established goals or resources for improving wellbeing, which greatly hampered efforts by employees hoping to make positive changes.[199] In contrast, growth and engagement metrics were tracked with precision, and were core to decision-making. As one engineer noted, if a proposed safety feature "drop[s] metrics, the key question will be by how much. Even a few minutes fewer means fewer ads and the impact on revenue at scale is significant."[200] Indeed, according to TikTok engineers, any proposed safety feature that results in "more than 1%" in "lost revenue" is unlikely to be approved. [201]

140. Employees who worked on child safety at TikTok frequently complained about being ignored. For example, Christina Crimmins, part of TikTok's Minor Safety ("MS") team, lamented to a colleague: "can't even describe to you the battles . . . Terrible. It feels like MS team is not

[194] Bejar Dep. at 150:12-16, 151:2-6.

[195] Bejar Dep. at 151:3-20.

[196] Bejar Dep. at 164:15-23.

[197] Bejar Dep. at 164:24-165:5.

[198] Bejar Dep. at 165:15 (emphasis added).

[199] TIKTOK3047MDL-002-00077113 at -136 (citing, as obstacles to improving wellbeing, "the lack of cross-functional cohesion caused by no shared definition of wellbeing and unclear decision-making processes, roles and priorities," and "a lack of resources and visibility" that made wellbeing work "mostly one-off, reactive, and [an inconsistent] priority across teams.").

[200] TIKTOK3047MDL-067-LARK-01027106, -110.

[201] TIKTOK3047MDL-042-LARK-00249728 at -728.

empowered to do anything but advise, and our advice can be ignored."[202] Other employees involved in well-being projects at TikTok stated that "the company prioritizes growth over all else in the short term rather than looking long term," and that a key barrier to the success of their well-being projects is the company "[p]rioritizing growth at all costs."[203]

141. A similar set of priorities were in place at YouTube. YouTube carefully monitored growth metrics, and built its systems around goals geared towards growth. As one YouTube executive explained, "all other things being equal, our goal is to increase (video) watch time," while "essentially ignoring the initial intention the user had when coming to YouTube if it helps to increase entertainment (measured via watch time)."[204] Stated another way, from YouTube's perspective, "[t]he objective of every view should be to drive the most long-term engagement with minimal user effort."[205]

142. In contrast to this laser-like focus on growth metrics, when YouTube finally, belatedly began introducing safety settings specific to teens in the 2020s – like bedtime reminders and break reminders – it did not undertake any meaningful evaluation of their effectiveness. YouTube engineers did not, for example, evaluate whether bedtime reminders caused kids to leave the app at bedtime, or whether break reminders caused kids to take breaks; nor did it set goals for those metrics.[206] Instead, they merely checked how many notifications were being sent, a meaningless metric when it comes to measuring effectiveness and user wellbeing.[207] A presentation from 2022 states this problem succinctly: "How are we measuring wellbeing? Current answer - we're not."[208] It was not until 2023 that YouTube introduced an AI model (VIBE) intended to track and address certain harms on the platform.[209]

---

[202] TIKTOK3047MDL-036-LARK-00107713713 at -714-15.

[203] TIKTOK3047MDL-004-00141860 (comments from employee Vai Pawha).

[204] GOOG-3047MDL-02185098.

[205] GOOG-3047MDL-02001804.

[206] *See* Goodrow Dep. at 457:25-458:23; Goodrow Dep. Ex. 37 at 31; Watson Dep.at 156:3-20; 254:3-255:34, Ex. 23.

[207] GOOG-3047MDL-02486605 at -605.

[208] Deposition of James Beser Vol. II, April 3, 2025, Ex. 62 at 42-43.

[209] VIBE (Volume Impacts Wellbeing), launched in 2023, is an algorithmic dispersion model that reduces concentration of content that can be harmful when shown in volume, such as social comparison and aggression. It was based, in part, on input from experts, and recognized that certain content – while not prohibited by YouTube community guidelines – are harmful to children when viewed in repetition/volume. *See, e.g.*, GOOG-3047MDL-02172004; GOOG-3047MDL-04882611. Although YouTube announced that VIBE would be applied to "teens in the United States," GOOG-3047MDL-00000258, it is in fact only applied to teens who have expressly declared themselves to be under 18 through the account creation process; teens who do not use YouTube through an account, or who misrepresented their age, do not benefit from

143. Snap also closely tracked user growth and engagement, investing heavily in features and data analytics to maximize daily active users and time spent on the app.[210] While a system for reporting issues existed, it was passive and reactive, lacking the same urgency and resources devoted to growth metrics.[211]

144. The result of these systems was predictable – safety features proposed by the Defendants' safety teams were rejected or watered down to the point that they had little impact. This is reflected in the adoption rates for those features, which in most cases were abysmally low.[212] The Defendants, in other words, were creating safety features that looked good on paper, but that very few people used and that did nothing to reduce excessive use of the platforms by kids. As one former Meta engineer put it, the company's safety features were a "placebo"; that is, "tools that sound good for regulators or people trying to pass legislation, but when you test the substance of it, they don't make teens' life meaningfully safer."[213] According to the engineer, "almost all of these [safety] tools do not do what they say they do on their pages."[214] Rather, they are "optimized to deal with PR fallout of hearings, news articles, testimony, and judgments."[215]

145. The Defendants have a deep understanding of how to push people to use features – the Defendants' engineers are "some of the most accomplished people in the world at creating products and features that people want to use."[216] They understood that "if you want somebody to use a feature, you put it in the front page. You make it responsive to touch on the user interface. You

---

VIBE. *See* Beser Dep. at 48:15-50:19. This is in contrast to the E.U., where VIBE is applied to declared and "inferred teens"; the age-inference model used in the E.U. to identify "inferred teens" has not been launched in the U.S. yet, despite its clear potential benefits. *See* GOOG-3047MDL-0571335; Beser Dep. at 60:11-62:17.

[210] Levenson Dep. Ex. 15; SNAP6022601.

[211] *See e.g.* SNAP0094503 (Snap employee explaining issues with Snap's reporting system have not been solved "due to technical challenges, privacy issues, and leadership in driving the effort"); SNAP1145380.

[212] *See, e.g.*, Meta's 6th and 7th Supplemental Responses to Plaintiff's Interrogatory 12; and TikTok's Objections and Supplemental Responses to Plaintiffs' Interrogatory Set 4.

[213] Bejar Dep. at 166:17-167:2; *see also id.* at 460:6-15 ("[S]afety tools and features on Instagram . . . were not effective at reducing the harm that people were experiencing on the platform.").

[214] Bejar Dep. at 550:5-10; *see also id.* at 597 ("But my experience of this is that – that these releases of a lot of these tools, they're as good as the paper that they're printed on, because when you test the tools -- and have many examples of this -- the tools do not live up to the promises that they are making to parents about what they do. And the timing of them seems to be optimized to deal with PR fallout of hearings, news articles, testimony, and judgments.").

[215] Bejar Dep. at 597:7-17.

[216] Bejar Dep. at 88:15-20.

point people at it. There [are] many things that are well-understood in the industry that you can do in order to drive feature discovery and usage."[217] The Defendants "could have made safety features and tools default features that kids had to use."[218] Instead, as discussed below, these features were often hidden in settings menus, not well-promoted, and not particularly effective even when used.

2. Real Usage Time Limits and Breaks

146. One of the most straightforward interventions for excessive use is to build in firm, enforceable time restrictions. Time restrictions can take different forms, but typically serve two different purposes – one is to limit the total amount of time that a child can be on the platform during a given day, and the other is to limit the hours of the day that the platform can be used, so that it is not available at times when it would interrupt sleep or interfere with school. (As Meta has acknowledged, "Nighttime social media use is associated with poorer mental health in teens due to displacing sleep . . . ; this is the most direct relationship between social media use and teen well-being."[219]) Other time limits build in required breaks after a certain amount of time on the platform, to interrupt long sessions.

147. Several applications have implemented time restrictions like these for accounts belonging to children. For example, the version of TikTok that ByteDance operates in China limits children under 14 to just 40 minutes of videos per day.[220] Under 14 accounts likewise cannot use the platform during normal sleeping hours, from 10 p.m. to 6 a.m.[221] Douyin has also introduced a mandatory 5-second pause between videos to reduce addiction.[222] None of these features, however, has been introduced in the U.S. This imbalance has led observers to criticize that TikTok "give[s] spinach to kids in China and opium to kids in America."[223]

148. While one might think that teen users would balk at such harsh restrictions, in fact evidence shows that there is a strong desire for them. TikTok summarized its findings from a focus group

[217] Bejar Dep. at 546:25-547:8.

[218] Bejar Dep. at 168:2-24.

[219] META3047MDL-003-00089142.

[220] "Chinese Short Video Apps Douyin and Kwai Introduce Feature to Cut Users' Screen Time," Krasia, (March 2019), https://kr-asia.com/chinese-short-video-apps-douyin-and-kwai-introduce-feature-to-cut-users-screen-time.

[221] "China: Children Given Daily Time Limit On Douyin- its version of TikTok," BBC (September 20, 2021), https://www.bbc.com/news/technology-58625934.

[222] "China's TikTok Adds Mandatory 5-Second Pause Between Videos," PC Mag, (October 22, 2021), https://www.pcmag.com/news/chinas-tiktok-adds-mandatory-5-second-pause-between-videos.

[223] TIKTOK3047MDL-004-00151118.

of teenagers, stating: "The majority of the teens express the need of being contained and they need limits imposed by something other than themselves. They imagin[e] some really drastic functions" like "a pre-set daily limit on the app (30 mins, or 1 or 2 hours), with the inability to reopen the app for a certain amount of time."[224] Surveys conducted by Meta similarly found that teens felt they were "spending too much time indulging in a compulsive behavior that they know is negative but [felt] powerless to resist."[225] Surveys conducted by YouTube likewise found that 45% of respondents "unintentionally stay on YT longer than they want."[226]

149. Defendants could have, and should have, implemented firm time limits for children's accounts on their platforms. Instead, they implemented soft "nudges" and other features that were typically opt-in, rather than default, and could easily be ignored by the user.

150. For example in 2018, Meta introduced a feature called "Time Spent Tools" that periodically reminded users of the amount of time they had spent on the platform, ostensibly to "give people more control over the time they spend on our platforms and also foster conversation between parents and teens about the online habits that are right for them."[227] However, as former Meta engineer Arturo Bejar has acknowledged, Meta "set[] up [this] tool for failure" in several ways.[228] First, the tool was made "opt-in," meaning that anyone wishing to use it "would have to navigate into settings to turn [it] on."[229] Meta has estimated the adoption rate to be at – around [redacted] – better than some of the safety features they introduced, but still far below what it would be if it was set as a default rather than opt-in setting.[230] Second, the tool did not actually create an enforceable time limit; instead it simply put up a reminder that the user could easily swipe away.[231] Perhaps most importantly, after the feature was implemented, Meta did not put any system in place to evaluate the tool's effectiveness and adjust it accordingly.[232] Without such a system, Mr. Bejar testified, the tool was little more than a publicity stunt.[233] Of course, if this system had been

[224] TIKTOK3047MDL-099-LARK-04759856 at -869.

[225] META3047MDL-003-00091414 at -420, -428; Gross Dep. at 76:13-81:25.

[226] GOOG-3047MDL-00236723 at Slide 11.

[227] Bejar Dep. at 558:11-560:10; Bejar Ex. 55.

[228] Bejar Dep. at 563:7-17.

[229] Bejar Dep. at 561:15-24.

[230] Meta's 6th Supp. Response to Plaintiffs' Interrogatory No. 12.

[231] Bejar Dep. at 560:22-561:7.

[232] Bejar Dep. at 562:16-563:6.

[233] Behar Dep. at 563:7-17.

implemented in an effective way, it would have reduced the time that teens spend on the platform, and therefore would have "decrease[d] the amount of money Meta makes."[234]

151. In 2022, Meta implemented a similar feature that allowed users to turn on "Take a Break" reminders to remind them when they have spent 10, 20 or 30 minutes on the app.[235] However, like the earlier "Time Spent" tools, this feature was opt-in, ensuring that few people would use it. Indeed, even though Meta purports to "proactively prompt teens to set reminders," the opt-in rate among teens for this feature as of April 2022 was just 0.152%,[236] and from January 8, 2023 through September 24, 2024 was only [redacted] for Youth users in the U.S.[237]

152. TikTok also announced a similar feature in 2022 known as "weekly digital well-being prompts" that would remind children of TikTok's screen time limit tool after they had used TikTok for more than 100 minutes in a day.[238] However, as originally implemented this was merely a notification of the tool's existence, not a default limit. In 2023, TikTok changed teen accounts to a default 60-minute daily time limit.[239] However, teens "can turn this setting on and off at any time."[240]

153. YouTube's time management tools were similarly ineffective as designed. For example, YouTube launched a "take-a-break" reminder and "time watched profile" in 2018,[241] and an opt-in "bedtime reminder" in 2020.[242] However, both of these tools were "opt-in" tools that had to be turned on by navigating through settings menus. [243] Moreover, none of these features acts as a hard stop – users can simply disregard the prompts.[244]

---

[234] Bejar Dep. at 150:12-16, 151:2-6.

[235] "Raising the Standard for Protecting Teens and Supporting Parents Online," Instagram Newsroom, (December 7, 2021), https://about.fb.com/news/2021/12/new-teen-safety-tools-on-instagram/.

[236] META3047MDL-040-00654288.

[237] Meta's Seventh Supp. Resp. to Interrogatory 12.

[238] *See* https://newsroom.tiktok.com/en-us/investing-in-our-communitys-digital-well-being.

[239] *See* https://newsroom.tiktok.com/en-us/new-features-for-teens-and-families-on-tiktok-us.

[240] Screen time, https://support.tiktok.com/en/account-and-privacy/account-information/screen-time.

[241] GOOG-3047MDL-00937887 at -914; 30(b)(6) deposition of James Beser, April 9, 2025, at Ex. 1.

[242] *See* Beser Dep. Ex. 1.

[243] Kim Depo. Ex. 11; GOOG-3047MDL-05713254.

GOOG-3047MDL-00000194 ("When you get a reminder, you can tap Dismiss to keep watching a video."); GOOG-3047MDL-00000116; GOOG-3047MDL-00000368.

154. Notably, all of the teen safety features referenced above depend on the platform knowing the correct age of the user. As discussed in more detail below, these platforms had no systems in place to verify a user's age. As a result, teens frequently sign up as adults, by simply entering an adult's birthday during sign-up.[245]

155. Snap has never implemented any time management tools.[246]

3. Gamifying Wellness, Not Just Engagement

156. Many of the addictive elements described above (streaks, likes, follower counts) effectively gamify the experience of the Defendants' platforms to ***reward engagement***. A safer, alternative approach – which the Defendants could have, and should have, implemented for minors' accounts – would be to ***gamify healthy behaviors***. Imagine if a social media app gave kids "reward badges" for taking breaks ("Nice, you took a 2-hour offline break!") or for using the app in moderation ("You stayed under 30 minutes today – achievement unlocked!"). Or if streaks were repurposed: instead of a streak for consecutive daily logins, how about a streak for consecutive days *logging off by 10 PM*, or a streak of doing a 5-minute meditation in the app each day? An app could likewise have a "Mindful Minutes" counter, awarding points when a user actually closes the app for a while or engages with well-being content. These points could unlock pleasant but non-addictive features like new profile themes or avatar customizations. At AngelQ, we have conducted some early research in this area and plan to deploy some of these techniques – we call them "light patterns" (to contrast them with the "dark patterns" used by the Defendants) – as a way to enhance the wellness of early users. Sadly, this should not be novel – it should have been standard practice already when dealing with kids.

157. Notably, there are many wellness apps that use gamification to encourage healthy behaviors. For example, Nike Training Club offers users incentives such as badges, streaks, and goal tracking to encourage users to workout consistently.[247] Headspace and Duolingo similarly encourage users to participate in daily healthy behaviors such as meditation or learning a new language by offering users the opportunity to earn achievement animations, earning experience points, and tracking accomplishments on leaderboards.[248]

---

[245] GOOG-3047MDL-04703742 at -742 ("only a small fraction of those who are actually u18 [under 18 years old] are declaring accurately" that they are under 18 during sign up); *see also* GOOG-3047MDL-01339056 at -071 ("[M]ost actual YT Teens users did not declare themselves between 13-17.").

[246] Snapchat Family Center, https://parents.snapchat.com/family-center.

[247] Nike Training Club, https://www.nike.com/id/ntc-app.

[248] How does the Run Streak Feature Work, Headspace,https://help.headspace.com/hc/en-us/articles/215730567-How-does-the-run-streak-feature-work; Duolingo Rewards,

158. The difference here is that those apps' end goals align with user benefit. Social media could have modified children's accounts to promote well-being rather than engagement, but that would require a paradigm shift in design philosophy. Thus, opportunities to **positively reinforce** breaks, self-care and moderation were largely bypassed.

4. Better User Controls

159. Another avenue for safer design is giving teens *more control* over what appears in their feeds. Typically, the algorithms decide that – often promoting the sensational or provocative because that drives engagement. A safer design would be to give teenagers **easy filters or knobs** to tune their experience.

160. For instance, a teen might be able to select a *"friend-focused mode"* that shows mainly posts from real-life friends rather than influencers. Or a teen might be able to tell the algorithm when they are recommended posts or videos that cause them distress, which could adjust the algorithm's ranking engine so that it is less likely to recommend such posts. This could be done in a way that is content-neutral, with a function that merely adjusts the algorithm without any need for either the platform or the algorithm to determine what type of content is being downgraded.

161. Empowering users with such choices would be a valuable safety feature: it would allow teens to reduce harmful "rabbit holes" and "filter bubbles" that algorithms frequently generate, when no user adjustments are available. The absence of these controls meant the platforms' recommendation engines could bombard a teen with undesired material and the teen had little recourse.

162. Technically, allowing users to tune the algorithm in this way is not hard. Some of the defendants have begun experimenting with content-neutral controls, though those changes have come far later than they should have. For example, in 2023, TikTok announced that users could "refresh" their feed – essentially resetting the algorithm.[249] And in 2022, Instagram introduced a "not interested" button that allows users to tag posts they are not interested in.[250]

163. Other, content-specific (non-neutral) controls introduced by the Defendants have been largely ineffective and, perhaps most concerningly, have given parents a false sense of security

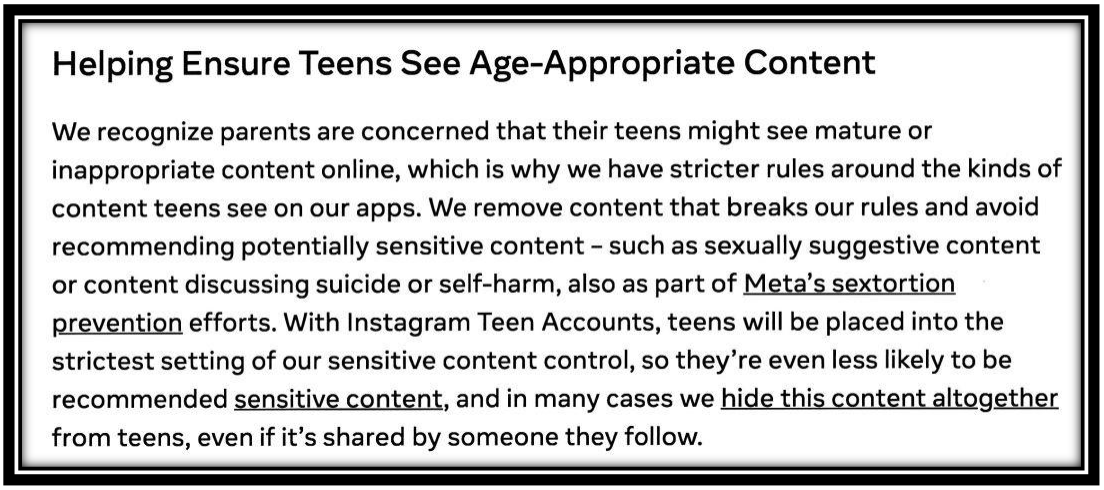
---

https://duolingoguides.com/duolingo-rewards/; How Duolingo Leaderboards Work, https://blog.duolingo.com/duolingo-leagues-leaderboards/.

[249] "TikTok Launches Tool to Retrain 'For You' Feed Algorithm," Medium, (March 20, 2023), https://medium.com/framedrop/tiktok-launches-tool-to-retrain-for-you-feed-algorithm-c97c7a4d38db.

[250] "Instagram 'Not Interested' Button Could Come to Save Your Feed," Digital Trends, (August 31, 2022), https://www.digitaltrends.com/social-media/instagram-not-interested-button-save-your-feed/.

about their children's use of the platforms. For example, in 2021, Meta introduced a "Sensitive Content Control." This feature was turned on by default for users under 16.[251] Meta advertised this feature as preventing Instagram's algorithm from "recommending potentially sensitive content – such as sexually suggestive content or content discussing suicide or self-harm."[252] An excerpt from Instagram's promotional literature is below:



Helping Ensure Teens See Age-Appropriate Content

We recognize parents are concerned that their teens might see mature or inappropriate content online, which is why we have stricter rules around the kinds of content teens see on our apps. We remove content that breaks our rules and avoid recommending potentially sensitive content – such as sexually suggestive content or content discussing suicide or self-harm, also as part of Meta's sextortion prevention efforts. With Instagram Teen Accounts, teens will be placed into the strictest setting of our sensitive content control, so they're even less likely to be recommended sensitive content, and in many cases we hide this content altogether from teens, even if it's shared by someone they follow.

Bejar Ex. 61 at 4

164. However, testing of this feature by Meta's former Product Leader for Site Integrity uncovered that, even with the so-called "sensitive content control" turned on, teen accounts were "recommended graphically violent, sexual, and other kinds of content."[253] A survey conducted in 2021, shortly after this feature was implemented, likewise found that 19% of children aged 13 to 15 reported seeing unwanted nudity or sexual images on Instagram in the last 7 days.[254]

165. In 2019, TikTok introduced a "Restricted Mode," based on the Teen Mode feature from TikTok's Chinese counterpart Douyin, that was intended to allow users to limit their account to content "Safe for General Audience."[255] Critically, however, it was made opt-in, and as a result it

[251] Introducing Instagram Teen Accounts: Built In Protections For Teens, Peace of Mind for Parents, Instagram Blog (September 17, 2024) https://about.instagram.com/blog/announcements/instagram-teen-accounts.

[252] Bejar Ex. 61 at 4.

[253] Bejar Dep. at 589:12-18.

[254] Bejar Dep. at 333:11-336:16.

[255] TIKTOK3047MDL-002-00101999 at -000.

was virtually unused. Internal documents from June 2021 state that the penetration rate for this feature was just 0.1 percent.[256] Nearly two years later, it was still at 0.11 percent.[257]

166. TikTok's own minor safety team, moreover, found that even when turned on, the Restricted Mode did not work as advertised. Rather, the content it featured was "often still too mature for that space, with Sexy Themes and Profanity being the largest offenders."[258] In a February 2021 employee group chat, Eric Ebenstein, TikTok public policy director, called the function "broken."[259] In a July 2021 employee group chat, [redacted], head of minor safety at ByteDance, similarly stated: "we need to do a lot to make sure Restricted Mode actually filters out inappropriate content because it's not meeting user expectations here."[260]

167. The Defendants should have ensured that these features functioned as advertised before misleadingly telling parents that their controls protect teens.

D. Conclusion

168. Numerous practical, often low-cost, content-neutral, safer design alternatives were available to the Defendants for years. These included modifying or removing addictive features, defaulting young users to strong privacy settings, and actively promoting user well-being through built-in tools. The consistent failure to adopt these alternatives – despite clear evidence of risk and even after internal acknowledgments of harm – shows a pattern of prioritizing maximum engagement and growth over the safety of minors. The Defendants chose designs that were known to be harmful to youth well-being when safer options were available.

[256] TIKTOK3047MDL-004-00147649 at -658.

[257] TIKTOK3047MDL-002-00101574 at -586.

[258] TIKTOK3047MDL-002-00101999 at -001.

[259] TIKTOK3047MDL-024-LARK-00035705 at -706.

[260] TIKTOK3047MDL-045-LARK-00447874 at -877; *see also* TIKTOK3047MDL-002-00077590 at Minor Safety Tab, Row 3 ("Despite the purpose of the existing restricted mode, a large amount of content (particularly with sexually suggestive or adult themes) that is not appropriate for minors is still not filtered out."); TIKTOK3047MDL-036-LARK-00111985 at -986 ("[C]urrent restricted mode lacks sufficient feed safety standards, posing high risks to users, which could result in potential PR issues and damage the brand's reputation. Improving the feed standards is critical to uphold the brand's reputation in the long run.").

VII. OPINION 2: DEFENDANTS' AGE VERIFICATION AND PARENTAL CONSENT SYSTEMS WERE BROKEN

A. Overview

169. Having failed to create a safe environment for children, the Defendants should have implemented systems to help parents protect children from the potential harms of their platforms. One of the most basic ways to protect children from adult-oriented platforms is a system of age verification and Verified Parental Consent (VPC). This ensures that children are not able to set up an account without some form of adult consent and supervision. It also allows the platform to exclude the youngest and most vulnerable children altogether.

170. Each of the Defendants purports to exclude children under the age of 13 from their primary social media platform. Some have gone further and indicated support for U.S. legislation that would require parental consent under the age of 16.

171. As described below, however, the Defendants failed to implement effective age verifications, and likewise failed to implement Verified Parental Consent. Typically, to determine the age of new users, the Defendants (at most) simply asked users to input a birthday or check a box confirming they are 13 or older. There was no real-time verification of identity, and no requirement of a parent's involvement. In other words, while they outwardly posted "No Under-13 Allowed" signs on the front door, they left the door unattended.

172. The results were predictable. Preteens swarmed these platforms en masse. Children lied about their birth dates, clicked a self-attestation box, and instantly joined the digital crowd. A 2021 survey of found that 38% of U.S. children aged 8 to 12 had used social media, and that 18% used it "every day," despite the platforms' rules prohibiting children under 13.[261]

173. In this section, I discuss how and why the Defendants' age verification and parental consent systems became a broken facade, chronicling each platform's failures to keep young children out.

B. The Need for Age Gating and Parental Consent Is Well-Recognized

174. Based on my experience, including my work setting up AngelQ, an online platform that provides a safer search and exploration experience to children, I have become intimately familiar with the legal requirements and best practices for providing online platforms to children.

[261] The Common Sense Census: Media use by Tweens and Teens, Common Sense Media, (2021) https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf at p.33.

175. Legislatures have long recognized that children merit special protection online, and statutes in both the U.S. and Europe impose heightened duties on those who design products or services that are used by kids, with varying age thresholds and restrictions.

176. For example, the Children's Online Privacy Protection Act (COPPA), in effect since 2000, provides that if an online service is "directed to children" under 13, or if it has actual knowledge that it is collecting personal information from an under-13 child, it must obtain Verifiable Parental Consent (VPC) and adhere to other safeguards.[262] VPC typically involves contacting the parent and having them provide proof of identity or payment information to confirm consent.[263]

177. More recent international regulations are stricter. For example, the EU's 2018 General Data Protection Regulation (GDPR) has a children's privacy provision requiring parental consent for processing personal data of children under 16 (with some member states choosing 13–15 as the cutoff).[264]

178. Notably, social media companies claim to support even stricter rules. Instagram,[265] Facebook,[266] Snapchat,[267] YouTube[268] and TikTok[269] all have terms of service that purport to prohibit children under 13 from joining at all (with our without parental consent). Meta has recently advocated for a rule in the U.S. that would require parental consent for children under the age of 16 (similar to the EU rule).[270] However, while the Defendants claim to support age verification and parental consent, they have failed to effectively implement it on their platforms.

179. A timeline of key U.S. and European regulations and their associated rules is below:

---

[262] 15 U.S. Code § 6501-06 (COPPA); *see also* Complying with COPPA: FAQ, FTC, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[263] Regulation (EU) 2016/679 (General Data Protection Regulation).

[264] Art. 8 GDPR; see also Consent to Use Data on Children, EU Agency for Fundamental Rights (https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children).

[265] Terms of Use, Instagram (https://help.instagram.com/581066165581870/).

[266] Terms of Service, Facebook (https://www.facebook.com/terms/).

[267] Terms of Use, Snap (https://www.snap.com/terms).

[268] Terms of Service, YouTube (https://www.youtube.com/t/terms).

[269] Terms of Service, TikTok (https://www.tiktok.com/legal/page/us/terms-of-service/en).

[270] Meta calls for parental control laws for under-16s, BBC (Nov. 16, 2023), https://www.bbc.com/news/technology-67433269.

1998	Congress enacts the Children's Online Privacy Protection Act (COPPA) in the U.S.
1999	**November 3:** The U.S. Federal Trade Commission (FTC) issues the first COPPA Rule.
2000	**April 21:** The initial COPPA Rule becomes effective in the U.S., requiring operators of websites/online services directed to children under 13 (or those with actual knowledge of collecting information from them) to provide notice and obtain verifiable parental consent before collecting personal information.
2013	**July 1:** Amendments to the COPPA Rule become effective, updating definitions and strengthening protections.
2018	**May 25:** The EU's General Data Protection Regulation (GDPR) becomes applicable. Article 8 sets the default age for a child to consent to the processing of their personal data for online services at 16, allowing member states to lower this to a minimum of 13. It requires controllers to make reasonable efforts to verify parental consent for children below the relevant age.
2020	**August 12:** The UK Information Commissioner's Office (ICO) issues the final Age Appropriate Design Code (AADC). **September 2:** The UK AADC comes into force, beginning a 12-month transition period for compliance.
2021	**September 2:** The 12-month transition period for the UK AADC ends, making conformance expected for online services likely to be accessed by under-18s in the UK. The code serves as a benchmark for GDPR compliance concerning children.
2025	**January 16:** The FTC finalizes the most recent updates to the COPPA Rule. **April 21/22:** The finalized amendments to the COPPA Rule are published in the Federal Register. **June 23:** The latest amendments to the COPPA Rule become effective.
2026	**April 22:** General compliance deadline for the latest COPPA Rule amendments (effective June 23, 2025).

C. Defendants' Failure to Implement Effective Age Gating and Verified Parental Consent

1. Facebook

180. Facebook, the first giant in this space, had a rule on paper that excluded children under the age of 13.[271] In practice, however, Facebook did essentially nothing to confirm anyone's age.[272] A child merely had to enter a birthday indicating that they were over 13 years old and an account was created, with full access to all features.[273] If someone under 13 entered their correct birthday, they were given a message indicating that they were not eligible to join the platform. However, upon receiving this message, they could simply try again by entering a different birthday.[274]

181. By 2011, it was already documented that over 7 million children under 13 had opened Facebook accounts by lying about their age.[275] More than 5 million of these users were under the age of 11.[276] Facebook's own terms were being violated at massive scale, effectively with the company's acquiescence.

182. More recently, after public pressure, Facebook has announced changes in policy that are nominally supposed to help remove under-13 accounts. However, the basic problem remains unchanged.

183. For example, in 2018, Facebook announced that its content reviewers would "lock" the accounts of "any underage user they came across," and "require the users to provide proof that they're over 13, such as a government-issued photo ID, to regain access."[277] In 2021, Facebook announced that it was developing AI tools to attempt to identify accounts belonging to children

---

[271] Facebook Changes Privacy Settings for Teens, CNN, October 31, 2013) https://www.cnn.com/2013/10/16/tech/social-media/facebook-teens-privacy.

[272] The Kids Who Lie About Their Age to Join Facebook, The Atlantic, (August 2016) https://www.theatlantic.com/technology/archive/2016/08/the-social-media-invisibles/497729/.

[273] *See, e.g.*, Instagram Still Doesn't Age-Check Kids. That Must change, Techcrunch, December 2019) https://techcrunch.com/2019/12/03/instagram-age-limit/.

[274] More than 80% of children Lie About Their Age to Use Sites like Facebook, The Guardian, (July 2013) https://www.theguardian.com/media/2013/jul/26/children-lie-age-facebook-asa.

[275] Underage Facebook Members: 7.5 Million Users Under Age 13, ABC News, May 9, 2011, https://abcnews.go.com/Technology/underage-facebook-members-75-million-users-age-13/story.

[276] Underage Facebook Members: 7.5 Million Users Under Age 13, ABC News, May 9, 2011, https://abcnews.go.com/Technology/underage-facebook-members-75-million-users-age-13/story?id=13565619.

[277] Facebook and Instagram Change to Crack Down on Underage Children, Tech Crunch, (July 19, 2018) https://techcrunch.com/2018/07/19/facebok-under-13/.

under 13.[278] Despite these announcements, however, Facebook continues to allow new users to create accounts without providing an ID, ensuring young children would continue to have easy access to the platform.

184. Perhaps more importantly, by the time these changes were made, Facebook's popularity with young children had greatly declined, as their attention shifted from Facebook to newer apps like Instagram. As outlined below, Instagram – also owned and operated by Facebook/Meta – had even laxer systems.

2. Instagram

185. Instagram, founded in 2010 and acquired by Meta in 2012, became wildly popular with preteens for photo sharing. It was "well-known at Meta in 2012 to 2015 that there were kids on Instagram who were under the age of 13."[279] In fact "that was one of the key reasons . . . for the Instagram acquisition"; Meta "wanted the very young kids on their social media apps."[280] An internal Meta memo noted, "the young ones are the best ones . . . you want to bring people to your service young and early."[281]

186. Though Meta was aware of the presence of young kids on the platform, from 2012, when Meta acquired Instagram, until December 2019, "Instagram did not ask kids for their age when they would sign up for an account." Meta employees referred to this as a "don't ask don't tell" policy, meaning "you know that there are kids under 13 there but you do not really talk about it and you don't ask about it. Like, if you didn't know somebody was under 13, then you didn't have to do anything about it." Meta's response to reports of underage users reflects this: in 2020, Meta had to create an underage enforcement war room to attempt to clear a backlog of more than 1.16 million reports. Considering how difficult it is to report, this is likely a small window into the true scope of the problem.

187. Even after Instagram began asking users for their age in 2019, it did not require any verification (such as an ID or credit card check). Meta's former Product Leader for Site Integrity, Arturo Bejar, acknowledged that it is "well-known in the industry" that kids can simply "lie [about their age] when they sign up for an Instagram or other social media account." Bejar testified that, during his time at Meta (through 2021), he "was not aware of any efforts to detect or remove under-

[278] How Do We Know Someone Is Old Enough to Use Our Apps?, Meta Newsroom, (July 27, 2021), https://about.fb.com/news/2021/07/age-verification/.

[279] Bejar Dep. at 185:24-186:3; *see also id.* at 112:15-18 (Q. "[W]hen you returned in 2019, . . . was it still an app that was very popular with young kids?" A. "Yes, it was.").

[280] Bejar Dep. at 185:10-22.

[281] [redacted] Dep. at 109:20-110:3

13 accounts." That was despite Mr. Bejar stating that Instagram "was not a safe place" for kids younger than 13.

188. According to Mr. Bejar, Meta had "the ability to build effective tools to try to prohibit kids younger than 13 from being on Instagram," but chose not to do so. This is confirmed by Meta's own admissions in this case. In sworn responses, Meta acknowledged that, "[p]rior to December 2019, Meta relied on a user's stated age from either their Facebook or Instagram account(s) (if available) to determine whether a user fell within an age group for age-based targeting; and if no such age information was available, Meta relied on a predictive age model to determine whether a user fell within a particular age group for ad targeting." If Meta had a predictive age model sufficient for purposes of ad targeting, surely it could have deployed that model to identify and kick off children under the age of 13 consistent with its stated policy.

189. Far from attempting to remove such accounts, Instagram "made it almost impossible to report underage accounts" and implemented "features that were designed to appeal to those kids." In a video I have reviewed from 2023, Mr. Bejar conducted an experiment where he set up a brand new account and watched Reels served by the Instagram algorithm. When a video of a child that appeared to be under 13 was shown, he would watch the video in full; for other videos, he would swipe quickly, without watching the full video. In less than a day, his feed was full of underage children, including many who were announcing their age on video as part of a popular viral trend. In other words, it was extremely easy to identify underage accounts on the platform, yet Instagram did not remove them.

190. In 2022, despite numerous lawsuits and a congressional investigation, Instagram's head of safety testified before the U.S. Senate that Meta still would not implement stricter age verification on the main app.[282] Instead, Meta's response was to start experimenting with optional tools – for example, in 2022 Instagram began testing a feature where a teen who tried to edit their birthdate from under 18 to adult would be asked to upload a video selfie for AI age estimation.[283] However, the system was not deployed more broadly. As currently implemented, it does nothing to identify kids who lied about their age the first time they tried to sign up. It also has not been deployed to identify pre-teens attempting to access the platform using a teenager's birthday. In essence, even by 2022, Meta only tweaked around the edges of age verification, despite years of evidence that the "honor system" was failing.

[282] Senate Hearing on Online Protections for Children, December 8, 2021, https://www.c-span.org/program/senate-committee/senate-hearing-on-online-protections-for-children/605914.

[283] Introducing New Ways to Verify Age on Instagram, Instagram Blog, (June 23, 2022) https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram.

3. Snapchat

191. Snapchat, launched in 2011, was practically designed to attract youth with its disappearing messages and fun filters.[284] Snapchat nonetheless adopted the same nominal age policy (13+) and the same ineffective verification as Facebook: self-reported birthdays.[285]

192. Snap's sign-up flow related to age is structured in a way that gives the appearance of compliance with minimum age requirements but lacks any substantive enforcement. When a user first opens the application and begins to create an account, they are prompted to enter their birthdate. By default**, Snap auto-fills the birthdate field with a year that corresponded to an age of 18 years**,[286] making it easy for users to proceed through the sign-up flow without making any adjustments to the birthdate.[287] This subtle design feature effectively prompts users to age themselves up. If the birthdate entered by a user corresponds with any age under 13, a soft error message pops up – "Sorry, looks like you're not eligible for Snapchat… but thanks for checking us out!" A user can then select "okay" to bypass the message, adjust their birthdate to an acceptable date, and proceed through the sign-up flow,[288] thereby allowing underage users to easily create accounts.[289]

193. In 2018 and 2021, Snap considered implementing a "cooldown period" to limit this practice.[290] The cooldown period would have required a potential new user to wait 5 minutes or 24 hours before trying to sign up again.[291] Snap, however, ultimately chose not to implement even this modest speed bump.[292]

194. Notably, Snapchat documents show that substantial numbers of under-13 kids were on the app. Snap, for example, has an internal age inference model for ad targeting and analytics. In December 2021, more than 43 million Snap users were internally identified by the company as

---

[284] Snapchat: The Biggest No-Revenue Mobile App Since Instagram, Forbes (November 27, 2012) https://www.forbes.com/sites/jjcolao/2012/11/27/snapchat-the-biggest-no-revenue-mobile-app-since-instagram/.

[285] SNAP0316064; SNAP6114428.

[286] Chan Dep11:18-118:14; Boyle 30(b)(6) Dep107:11-108:19; SNAP2268193.

[287] SNAP6398196; SNAP4571055.

[288] Chan Dep. 216:16–223:15; Boyle 30(b)(6) Dep162:19-164:20.

[289] Boyle 30(b)(6) Dep Ex. 6. Boyle 30(b)(6) Dep. 165:7–169:8, Feb. 26, 2025.

[290] SNAP5708527; SNAP5490201; Boyle 30(b)(6) Dep. 179:18-180:11; Chan Dep215:15 - 223:15; 218:13-224:22.

[291] SNAP5490201.

[292] *Id.*

under 13 years old.[293] Third party studies have reached similar findings. A Common Sense Media research study found that by 2021, 13% of 8–12 year-old "tweens" in the U.S. said they had used Snapchat at least once.[294] (Instagram was not far behind, with 10% of tweens reporting having used Instagram despite being below the allowable age.)[295]

195. Internal communications at Snap from 2022 tellingly state: "I don't think we can say that we actually verify users' ages," acknowledging that any kid who can type a fake birthdate can access the platform.[296] During a UK parliamentary hearing, Stephen Collins, a Snap executive, testified that their age-related safeguards are "effectively useless" in preventing underage users from accessing the platform.[297]

4. TikTok

196. TikTok's predecessor, Musical.ly, was founded in 2014 as a viral video app hugely popular with grade-school children for singing and dancing clips.[298] From 2015 to 2018, the app did not even ask for a user's age at signup. Children of any age could download Musical.ly, make an

[293] SNAP7292616.

[294] Common Sense Media, The Common Sense Census: Media Use by Tweens and Teens, (2021) https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf at 5.

[295] Reports from March 2019 detail testimony by Stephen Collins, then Snap's Senior Director of International Public Policy, before the UK's Digital, Culture, Media and Sport committee. Collins acknowledged that Snapchat's age verification was not foolproof and could be bypassed. *See, e.g.*, Christine Fisher, "Snapchat admits its age-verification system doesn't work," Engadget, March 20, 2019, https://www.engadget.com/2019-03-20-snapchat-uk-parliament-age-verification.html; The Independent, "Snapchat admits its age verification system does not work,", https://www.independent.co.uk/tech/snapchat-age-verification-not-work-underage-ageid-a8829751.html; Sky News, "Snapchat admits age verification failures to MPs," March 19, 2019, accessed May 10, 2025, https://news.sky.com/story/snapchat-admits-age-verification-failures-to-mps-11670399.

[296] *Id.*

[297] *Id.*

[298] How a failed education startup turned into Musical.ly, the most popular app you've probably never heard of, Business Insider, (May 28, 2016) https://www.businessinsider.com/what-is-musically-2016-5.

account with just an email or phone number, and immediately start creating and sharing videos publicly.[299]

197. In 2018, Musical.ly was acquired by ByteDance and merged with ByteDance's TikTok. ByteDance choose to purchase Musical.ly to kick start its US operations despite Musical.ly's primary userbase being 7-12 year old girls.[300] These children automatically became TikTok users when the app updated on their phones.[301] By 2019, TikTok was the subject of an FTC complaint for its collection of personal data from thousands of children under the age of 13 without parental consent.[302] The case resulted in a then-record $5.7 million fine.[303] The FTC Chairman noted in that case: "The operators of Musical.ly knew many children were using the app but they still failed to seek parental consent," calling the violation "flagrant."[304] In other words, TikTok's leadership was on clear notice as of 2019 that its age verification was flawed.

198. TikTok promised changes, and in 2019 it rolled out a segregated "under-13 mode" – essentially a watered-down version of TikTok that one can access if they admit at signup to being under 13.[305] Tellingly, however, this was still based purely on self-reported age. Any child could falsely enter an older birth date to bypass the restricted mode.[306] TikTok's under-13 mode was thus a cosmetic solution; the main app remained wide open. TikTok was well aware its "age gate" was ineffective in preventing children from using TikTok.[307] Even as late as 2023, TikTok reported

---

[299] *See, e.g.,* Who's Too Young for an App? Musical.ly Tests the Limits, New York Times, (September 16, 2016) https://www.nytimes.com/2016/09/17/business/media/a-social-network-frequented-by-children-tests-the-limits-of-online-regulation.html.

[300] Kirchhoff Dep. at 65:12-66:21, 106:1-107:13.

[301] Kirchhoff Ex. 7.

[302] Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law, Federal Trade Commission, (February 27, 2019) https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy.

[303] *Id.*

[304] *Id.*

[305] Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law, Federal Trade Commission, (February 27, 2019) https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy.

[306] Miller Dep. at 151-152, 181.

[307] TIKTOK3047MDL-024-LARK-00026909 (Minor Safety SWOT analysis reporting internally that "age gate and identification, though compliant, is easy to circumvent"); TIKTOK3047MDL-021-LARK-00005510 (Age-gate is "a feeble safety precaution"); TIKTOK3047MDL-072-LARK-01117815 (In May 2020, TikTok's Global Head of Trust and Safety reported "Re age verification efforts for now: 1) Currently, using age gate as the major approach - and we all know

internally that 96.1 million U.S. users were on TikTok without a birthday, and 20.5 million of those users were actively using the platform.[308]

199. Even more alarmingly, TikTok documents show it sought to "reduce the # of existing users that need to go thru the age gate to minimize business impact."[309] TikTok decided not to ask users for their birthdays at all "as long as their account are associated with facebook or google."[310] This loophole continued until well into 2022.[311]

200. Even in 2022, TikTok continued to mull over whether it should promise to remove all users under 13, noting that doing so would result in "Less DAU" because "some parents use our app because their children are using it" and "When kids use other apps, they will keep using them after they grow up."[312]

201. Internal data and independent surveys confirmed substantial usage by under-13 children on TikTok, in violation of the official policy.[313] For example, Thorn's 2020 study, which it shared with TikTok, found that 33% of 9–12 year-olds report using TikTok daily.[314] In 2021, TikTok estimated internally that it had 4,758,841 users under 13 accessing TikTok in the United States (37,674,162 globally) and that around 370,000 new users under 13 created TikTok accounts every day.[315] Even though hundreds of thousands of users admitted in their account bio statement that

---

why it is not comprehensive and effective"); TIKTOK3047MDL-015-00343407 ("Users are likely to falsify (lie) about their ages" and noting "the distribution of users' birthdates should resemble the distribution of birthdates of the general population. However, that's not the case, implying that users falsify their birthdates. January 1st is the most common birthday among TikTok LIVE hosts, even though it is one of the most uncommon birthdays in the general US population.").

[308] TIKTOK3047MDL-002-00102033 at -036.

[309] TIKTOK3047MDL-098-04150329; TIKTOK3047MDL-039-LARK-00215256 ("Yes the frustrating issue is the lack of concern that we are reaching underage users that haven't input the age gate. This is illegal in the US and many other markets, and can have disastrous outcomes if clients become aware of this.").

[310] TIKTOK3047MDL-098-04150331; TIKTOK3047MDL-098-04150330.

[311] Han Ex. 45.

[312] TIKTOK3047MDL-004-00290427.

[313] *See, e.g.*, Maher Ex. 4 ; TIKTOK3047MDL-087-LARK-03254375; TIKTOK3047MDL-042-LARK-00237491.

[314] TIKTOK3047MDL-028-00806247; TIKTOK3047MDL-028-00806246.

[315] TIKTOK3047MDL-042-LARK-00237491. In the same document, TikTok estimated that 24,294,463 users under 16 were accessing TikTok's livestreaming feature in violation of its stated policy. *See also* TIKTOK3047MDL-038-LARK-00192063 ("10% of users are underage");

they were under age (*e.g.*, "I am 7 years old"), TikTok made a policy decision not to proactively detect and ban those users.[316]

202. Further demonstrating the issue, TikTok's age gate data showed 11 million more users on TikTok listed in the 18- to 24-year-old category *than existed in the United States* according to census data, which led TikTok to the obvious conclusion that "age gate is not accurate in 18-24."[317]

5. YouTube

203. YouTube has long been the most popular website for children – a fact Google brags about to advertisers. Internal presentations to toy companies touted YouTube as "today's leader in reaching children age 6–11" and "the #1 website regularly visited by kids."[318] Yet, Google simultaneously claims to regulators that YouTube is not "directed to children" and that children only should be on a separate YouTube Kids app.[319] In reality, YouTube collects data on children viewing kid-oriented channels on the main platform and serves them targeted ads, reaping millions in revenue.[320]

204. There are numerous holes in YouTube's purported age verification systems. For one, the YouTube website and app are accessible to users ***without signing up for an account***; as a result,

---

TIKTOK3047MDL-021-LARK-00006866 (In 2023, there are "1.1m users who all figured out how to bypass the age gate," with an employee asking "Why are 1.1m people smarter than us").

[316] Classen Dep. at 197:18-201:14 (TikTok employee noting "if you are admitting your age as 7, why even spend a brain cell to find a way to allow you to appeal?" and "This is how obvious it is. We are not even trying to detect them smartly."); TIKTOK3047MDL-153-LARK-07399033; TIKTOK3047MDL-044-00839323 ("TikTok does not use any methods to proactively detect and age correct users who are between the ages of 13 to 17 who have lied at the age gate saying they are over 18," users it refers to as "hidden minors").

[317] TIKTOK3047MDL-153-LARK-07399033; TIKTOK3047MDL-079-LARK-02273249 at -250 ("We have 2X accounts for 18-24 female comparing to Us census."); TIKTOK3047MDL-090-LARK-03712197 (admitting in January 2023 that "most likely 40% of 18-24 are actually 13-18").

[318] Google, YouTube To Pay $170 Million Penalty Over Collecting Kids' Personal Info, NPR (September 4, 2019) https://www.npr.org/2019/09/04/757441886/google-youtube-to-pay-170-million-penalty-over-collecting-kids-personal-info.

[319] Youtube Kids, YouTubeyou're your Child's Google Account, https://support.google.com/youtubekids/answer/7124142?hl=en-gb.

[320] Google, YouTube To Pay $170 Million Penalty Over Collecting Kids' Personal Info, NPR (September 4, 2019) https://www.npr.org/2019/09/04/757441886/google-youtube-to-pay-170-million-penalty-over-collecting-kids-personal-info.

so-called "logged out" users – *i.e.*, users that are not signed into an account – are not age verified in any way.

205. Even for users who do create an account, YouTube – like the other Defendants' platforms – simply asks them to enter their birthday during the sign-up process.[321] The "declared age" entered during sign-up drives all of YouTube's recently integrated safety features for children, including (for example) "break" reminders and modifications to the recommendation algorithm. In other words, children who lie about their age immediately bypass all of these safety features.

206. Even for "logged in" users, YouTube did not require everyone to enter a birthdate; some sign-up methods (*e.g.*, using an Android phone prior to 2018) did not require a birthdate, resulting in hundreds of millions of "Age Unknown" accounts on the platform.[322] Age-unknown accounts are treated as "adults," with the exception of age-gated (18+) content.[323]

207. As YouTube internal documents note, "only a small fraction of those who are actually u18 [under 18 years old] are declaring accurately."[324] Thus, "[d]eclared isn't a reliable signal."[325] Indeed, Google avoids using declared age for targeted advertising and for algorithmic recommendations. Instead, for advertising and recommendations, Google uses inferred age models that estimate a user's age based on, among other things, their activity on the platform and other data sources.[326]

208. YouTube's purported fixes for these issues have been ineffective. Beginning in 2019 YouTube introduced something called the "Athena Classifier," a machine learning system to identify channels likely to be controlled by unsupervised under-13 users.[327] However, this system is extremely limited in several ways. First, [redacted].[328] Second, [redacted]

[321] *See, e.g.*, GOOG-3047MDL-04585554 ("In the United States and most of the ROW [rest of the world], YT [YouTube] currently relies on declared age. However, in 2024, we are likely to have to start inferring or verifying user age in some states unless recently passed laws are successfully contested in court.").

[322] GOOG-3047MDL-05705953 at -953 (estimating 650M age unknown accounts as of 2019).

[323] *See* Beser Dep. 105:21-105:3.

[324] GOOG-3047MDL-04703742 at -742; see also GOOG-3047MDL-01339056 at -071 ("[M]ost actual YT Teens users did not declare themselves between 13-17.").

[325] GOOG-3047MDL-04683365 at -366; *see also* GOOG-3047MDL-03385518 at - 518.

[326] *See, e.g.*, Hebda Dep. at 48:7-14, 59:18-20, Saphir Dep. at 34:6-3, 35:2-25.

[327] GOOG-3047MDL-01342809.

[328] *See* JainDep. Ex. 1 at 5.

[redacted][329] As a result, [redacted].[330] By that time, [redacted].[331]

209. YouTube was charged by the FTC in 2019 with systematically violating COPPA. In response to the FTC's action, Google paid a $170 million fine and agreed to implement new policies. Even after that fine, however, Google still did not require verification of age or identity for users creating a YouTube account.

210. After 2019, YouTube did disable many behavioral ads and comments on content labeled as "made for kids," and it launched a supervised account option for young teens. Yet, the fundamental signup process on Google's services remained a simple birthdate entry. A 10-year-old could make a Google account claiming to be 15 and immediately access YouTube's entire library (aside from age-restricted adult videos) with minimal friction. In short, even after paying hefty fines, YouTube's approach to age gating barely changed where it truly mattered – at the point of entry.

211. A 2020 survey by the nonprofit Thorn found that a whopping 78% of kids aged 9–12 were using YouTube on a daily basis (by far the highest of any online platform).

6. Mounting Evidence, Lawsuits and New Positions on Legislation.

212. As the pandemic pushed kids' screen time to new heights, studies began quantifying the obvious: enormous numbers of children under 13 were active on social media despite the age restrictions. A 2021 national survey by Common Sense Media found 38% of tweens (ages 8–12) had used social media, a jump from 31% just two years prior.[332] Remarkably, 18% of 8–12 year-

[329] *Id* at -810.

[330] GOOG-3047MDL-01342809 at 812 ("Today [2023], underage accounts that are actioned by Athena are generally [redacted]").

[331] *Id* at -813. ("[redacted].").

[332] Common Sense Media, The Common Sense Census: Media Use by Tweens and Teens, (2021) https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf at 5.

olds were using social media every day.[333] These children should not have been able to create accounts at all, yet millions had done so.

213. By late-2021, Congress and regulators demanded that executives from the Defendants appear for hearings. The Senate Commerce Committee's subcommittee on consumer protection held sessions in the fall of 2021 and questioned Facebook, Snapchat, and YouTube executives over child safety. Lawmakers were incredulous that these multibillion-dollar tech companies, with all their ingenuity, still relied on laughably weak age checks. As Senator Mike Lee pointedly demonstrated in that hearing, his staff created a test Snapchat account for a fictitious 15-year-old, provided no additional info, and were "immediately bombarded with wildly inappropriate content" on Snapchat's Discover page – including invitations to an 18+ sex-themed game – all of which would be visible to a child under 13 who lied about their age.

214. These hearings were followed by a wave of legal actions by state Attorneys General. In 2023, a coalition of 33 states sued Meta – lawsuits which I understand have been coordinated with this case – alleging in part that Meta knowingly allowed and profited from underage users on Facebook and Instagram.[334] A number of states also sued TikTok around the same time, alleging that the company addicted and harmed underage children.[335] And in 2024, Florida's Attorney General sued Snapchat for violating a new state law by not obtaining parental consent for 13- to 17-year-old users and by continuing to allow under-13 users despite knowledge.[336]

215. Subsequently, the companies started to retreat from their long-held laissez-faire approach. In 2023, Meta began talking about support for federal digital ID legislation to verify ages online – a sharp reversal from its earlier lobbying. [337] Meta nonetheless declined to implement age verification requirements in the U.S. unilaterally.

---

[333] *Id.*

[334] Meta sued by 33 state AGs for addictive features targeting kids, NBC News, (October 24, 2023) https://www.nbcnews.com/tech/tech-news/meta-sued-33-state-ags-addictive-features-targeting-kids-rcna121927.

[335] TikTok sued by 14 attorneys general over alleged harm to children's mental health, CNN, (October 8, 2024) https://www.cnn.com/2024/10/08/tech/tiktok-sued-14-states-childrens-mental-health.

[336] Florida attorney general sues Snapchat, claims it's violating state's social media law, CBS News, (April 23, 2025) https://www.cbsnews.com/miami/news/florida-attorney-general-sues-snapchat-claims-its-violating-states-social-media-law/.

[337] *See e.g.* Big Tech Knows that Age Verification is Necessary, The Hill (September 7, 2023) https://thehill.com/opinion/congress-blog/4192462-big-tech-knows-that-age-verification-is-necessary/.

216. YouTube announced in 2025 that it planned to implement a machine learning system to try to identify underage accounts.[338] These steps, however, came after more than a decade of what can only be described as willful blindness. As I will explain in the next section, the technology and methods to enforce age limits have long been available. The failure was never due to technical impossibility; it was a failure of will and incentive.

VIII. OPINION 3: REAL AGE CHECKS AND PARENTAL PERMISSIONS HAVE BEEN AVAILABLE FOR MORE THAN A DECADE

217. When confronted (by reporters, researchers, or lawmakers) about the large numbers of under-13 children on their platforms, social media companies have frequently fallen back on the excuse that effective age verification was too difficult or simply impossible to implement. For example, in response to a 2011 Consumer Reports finding that 7.5 million U.S. children under the age of 13 had Facebook accounts, Facebook responded by claiming "it is not easy for an online company to enforce age limits . . . . [T]here is no single solution to ensuring younger children don't circumvent a system or lie about their age."[339] Other arguments raised included that requiring ID or credit card verification for every user would invade privacy or exclude people without IDs, and that kids would always find a way around restrictions.[340]

218. As outlined below, robust systems for online age checks and parental consent were readily available during that time period and are available today. Standard tools include credit card verifications, ID scans, and AI age estimators (among others). These tools were widely in use in other industries, including (for example) by video game console manufacturers and mobile operating system developers. Platforms like Microsoft's Xbox Live, Nintendo's online network, Sony's PlayStation Network, Apple's iOS ecosystem, and Google's Android system have been successfully verifying parent permission and supervising child accounts for more than a decade. In short, age verification and parental consent online has been the norm across much of the tech and media industry.

219. Defendants' failure to implement effective age checks and parental consent was not reasonable and not in-line with industry standards, including the standards set for children under the age of 13 by COPPA.

---

[338] YouTube Blog: Big Bets for 2025; Saffel Dep. Ex. 1.

[339] Underage Facebook Members: 7.5 Million Users Under age 13, ABC News, (May 9, 2011) https://abcnews.go.com/Technology/underage-facebook-members-75-million-users-age-13/story.

[340] *See, e.g.*, How Do we Know Someone is Old Enough to Use Our Apps?, Meta (July 27, 2021) https://about.fb.com/news/2021/07/age-verification/.

A. Widely Available Age Verification Tools

220. Modern digital platforms have had a rich toolkit of age verification methods at their disposal for many years that do not unnecessarily harvest personal data. Examples of such technologies include the following:

1. Credit Card and Payment Verification (2010 to present)

221. One of the oldest and simplest methods to verify age is the credit card check. Credit cards (as well as debit cards in adult-controlled contexts) serve as a proxy for adulthood because minors generally cannot obtain one independently. As early as 1999, the U.S. FTC explicitly endorsed "the use of a credit card . . . in connection with a monetary transaction" as an approved method of parental consent under COPPA.[341] In practice, this typically means placing a small, temporary charge (on the order of $0.50–$1.00) on a parent's card to confirm an adult is present and consents. The amount is trivial and often refunded or donated to charity, serving only as a test of card ownership.

222. Importantly, the platform does not need to store the card information or charge anything beyond that token amount. The goal is simply to piggyback on the banking system's existing age vetting. If you have a valid credit card in hand, you are highly likely to be an adult or acting with one's supervision.

223. Nintendo has used this method since 2012, charging a one-time $0.50 fee to create a Nintendo Network account for a child, as "proof of consent . . . in accordance with COPPA."[342] Credit card info was not stored after verification.[343] Microsoft and Sony implemented similar measures for their gaming networks. Microsoft's Xbox Live has required an adult to verify a child's account with a small card charge or equivalent since 2013, and Sony updated the PlayStation Network in 2017 so that the first time a user set up a family adult account, a $0.50 charge is made "to verify that you are an adult."[344] Apple similarly adopted this approach when it

[341] Complying with Coppa: Frequently Asked Questions, FTC, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#I.%20Verifiable%20Parental%20Consent.

[342] Why Am I Prompted to Enter a Credit Card to Create a Nintendo Account for My Child, https://en-americas-support.nintendo.com/app/answers/detail/a_id/1334/~/why-am-i-prompted-to-enter-a-credit-card-to-create-a-nintendo-account-for-my.

[343] *Id.*

[344] How to Set Parental Controls on the PlayStation 4, Common Sense Media, (March 15, 2021) https://www.commonsensemedia.org/articles/how-to-set-parental-controls-on-the-playstation-4.

rolled out Family Sharing in 2014: if a parent wants to create an Apple ID for a child under 13, Apple requires a credit card CVV code as part of verifying parental consent.[345]

224. In short, any platform that genuinely wanted to keep children off adult services (or obtain parental consent) had a ready-made solution: ask for a 50-cent card verification. This method was effective and widely understood by consumers. It balances privacy and security – the platform learns nothing more than that a valid adult payment method was used, and regulators like the FTC have considered this "reasonably calculated" to confirm a parent's identity.

225. At one point, Meta recognized credit card collection as an effective method for parental consent and age verification. In 2010 Meta began to work on Project Kid, a version of Facebook meant for those under age 13.[346] This project required various levels of parental consent to be COPPA compliant, and included an option where parents had to enter a credit card to give consent.[347] Project kid did not go forward, but Meta never transferred this clearly feasible form of verification to their main app.

META3047MDL-044-00097840

226. **Pros:** Very high accuracy (hard for a child to fake owning a credit card); low cost per verification (pennies) with industry infrastructure already in place; no retention of sensitive data needed beyond a transaction record.

227. **Cons:** Not every parent has a credit card or is willing to use it online (some use debit or none at all, though alternatives like a nominal charge to a mobile phone bill could be offered).

---

[345] Create An Apple Account for Your Child https://support.apple.com/en-us/102617.

[346] META3047MDL-034-00385870.

[347] META3047MDL-044-00097840.

Nonetheless, multiple options exist if a parent doesn't have a card – Microsoft, for instance, allows an adult to contact customer support and verify with a government ID instead.[348]

228. Overall, credit card verification has been a feasible, affordable solution since at least the early 2010s, and companies like Nintendo, Sony, Microsoft, Apple, Google, and Niantic (makers of Pokémon GO) have all utilized it to comply with child safety laws. Those use cases demonstrate that this method works at scale. Moreover, the cost and friction are minimal, as evidenced by parents routinely completing these verifications within minutes.

2. Government ID Scanning and Database Checks (2012 to Present)

229. Another highly effective method available for years is scanning an official ID (driver's license, passport, etc.) and verifying the birthdate. By 2012, services like Jumio and Veratad offered SDKs to scan an ID with a smartphone camera and automatically parse the data for age verification.[349] The COPPA rule was updated in 2013 to explicitly allow "checking a government-issued identification against databases, provided the ID is deleted after verification."[350] Many online alcohol and tobacco retailers, for instance, have used third-party identity verification services to confirm age before shipment, leveraging DMV or credit bureau databases.[351] Dating apps and sharing economy platforms also commonly verify IDs to ensure users are adults or authentic.[352]

230. The technical process is straightforward: a user is prompted to take a photo of their driver's license or passport; the image is either analyzed locally or sent securely to a verification service.[353] The service extracts the birth date and checks that the ID is valid (sometimes cross-referencing public records or hologram patterns). The image can then be deleted, and only an "age verified" flag or the birth date is kept.[354]

---

[348] Getting Started With Microsoft Family Safety, https://support.microsoft.com/en-us/account-billing/getting-started-with-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344.

[349] https://www.jumio.com/faq; https://veratad.com/methods/identity-documents.

[350] Bumble Rolls Out ID Verification in Dating App Safety Push, Yahoo Finance, (March 17, 2025) https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business.

[351] *See e.g.*, https://ideausher.com/blog/how-does-drizly-work/.

[352] *See e.g.*, https://finance.yahoo.com/news/bumble-rolls-id-verification-dating-120000362.html.

[353] *See, e.g.*,Veratad, https://veratad.com/solutions/age-verification.

[354] Age ID Verification FAQ, https://en.help.roblox.com/hc/en-us/articles/4407276151188-Age-ID-Verification-FAQs.

231. Costs are modest: there are numerous vendors (Jumio, Veriff, Onfido, etc.) offering automated ID checks for around $1 or less per verification.

232. **Pros:** Very high confidence in age if ID is legitimate; a one-time process that can be tied to the user's account; can be combined with face matching (selfie vs. ID photo) to prevent use of a stolen ID.

233. **Cons:** Slightly higher friction – requires the user (or parent) to have an ID and be willing to share an image of it. There are also privacy concerns if not handled correctly (since an ID has sensitive info like full name and address). However, those concerns can be mitigated by automatically deleting or redacting the ID data after age verification is complete. Indeed, COPPA-compliant implementations mandate deletion after verification to protect privacy.[355]

3. Federated Identity and Single Sign-On Systems (2014 to Present)

234. Another solution that has been available is leveraging federated identity providers – in simpler terms, using a trusted third party to vouch for a user's age. Examples of this are websites that let you "Log in with Google" or "Log in with Apple." These logins (OpenID Connect/OAuth standards, widely adopted by 2014) can carry additional attributes, like an "age over 18 verified" token, if the identity provider has that info. For example, Apple's system, as of iOS 15 (2021), allows an adult user to store a state ID or driver's license in their Apple Wallet.[356] Apple can cryptographically confirm to a requesting app that "Yes, this user's ID in Wallet shows they are over 21" without revealing the actual birthdate or ID details. This is an implementation of anonymous credentials or "zero-knowledge proofs" – concepts available in academic and enterprise identity systems for years (Microsoft's U-Prove and IBM's Idemix were offering such tech in the early 2010s).[357] In the context of children's safety, a federated approach could mean, for instance, that a child tries to sign up for Instagram and is given an option: "Have your parent sign in with their Google/Apple account to approve your age." The parent's account, which is already verified as an adult (since Google and Apple both require credit card or ID for family accounts), would then signal the okay. This is very similar to how Family Link (Google) or Family Sharing (Apple) already function for creating child accounts in their ecosystems. In fact, any user under 13 on an Android device cannot create a standard Google account; the parent must consent via their own Google credentials and a verification step. While Google used this feature for many Google services, it did not utilize it for YouTube.

---

[355] Complying with COPPA: Frequently Asked Questions https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[356] Add Your Driver's License to Apple Wallet, https://support.apple.com/en-us/111803.

[357] Almeida, Barbose, Bangerter, Full Proof Cryptography: Verifiable Compilation of Efficient Zero-Knowledge Protocols at 3.

235. Standards for sharing age attributes existed by 2014, and companies like Microsoft and Google were part of initiatives (*e.g.*, the Kantara Initiative, the FIDO alliance) exploring these identity claims for age.[358]

236. **Pros:** Federated and single sign-on methods can make age verification nearly frictionless – you click one familiar button (log in with X) and the rest is handled through back-end communication. If major identity providers cooperate, users wouldn't need to repeatedly prove age for every service – do it once with a trusted entity, and reuse that trust.

237. **Cons:** It requires coordination with third parties. A single social media company could not unilaterally implement this without cooperation of another company that performs the age verification.

4. Mobile Carrier Age Attributes (2015 to Present)

238. This method is closely related to federated identity, but has certain unique advantages. Mobile carriers know the identity of their subscribers – you typically have to provide ID or a credit check to get a SIM card or phone plan, or at least you have a billing relationship. In some regions, carriers explicitly record birthdate or have a flag if a user is a minor. Carriers in the UK, for example, have long enforced adult content blocks: a mobile user must prove age (usually in store or via credit card) to lift the content filter on 18+ websites.[359] This means the carrier has a database of which accounts are verified 18+. They expose a simple mechanism (like sending a text or making an API call) for websites to query that. A service can thus say, "Charge 1 cent to the user's mobile bill to verify they are adult – if the carrier approves the charge, it's an adult account" (similar in concept to credit card, but using phone billing). In fact, standards like the aforementioned Age Verify API through Mobile Connect allow exactly that: a third-party service can request the mobile network to confirm age attributes. The user consents (typically via a prompt or by responding to an SMS), and the carrier returns a yes/no on the age check.

239. This method was feasible and in commercial use by 2015. It is more prevalent in Europe and Asia where carriers have been more proactive on identity services. U.S. carriers have been slower to deploy consumer-facing age verification APIs, but they do offer phone-based identity verification for fraud prevention that includes subscriber info. There is no technical barrier to using phone ownership as an age signal. After all, many social media accounts are tied to phone numbers for SMS verification – meaning platforms are already interfacing with carrier networks (for

[358] Fido Alliance, https://fidoalliance.org/; https://kantarainitiative.org/kantara-initiative-and-iiw09-its-all-about-collaboration/.

[359] *See e.g.*, https://www.three.co.uk/support/internet-and-apps/accessing-and-blocking-adult-content; https://www.o2.co.uk/help/safety-and-security/keeping-safe-online/age-restricted-content-and-age-verification.

sending codes) but not leveraging the additional data they could. To protect privacy, the exchange could be as minimal as "Subscriber of this phone number is age > 18: true/false."

240. **Pros:** Uses something nearly everyone has (a phone); no extra apps or scans needed – it can be as simple as ticking a box during sign-up saying "verify via my mobile account" and the carrier confirms in background.

241. **Cons:** It may not catch a scenario where a child is using a phone plan under their parent's name (the carrier may only have the adult's info). Carrier verification could be offered alongside other methods to cover edge cases.

5. AI-Based Facial Age Estimation (2018 to Present)

242. A significant development in recent years is the rise of AI facial age estimation. This technology uses computer vision algorithms to analyze a photo or video selfie and output an estimated age – without identifying the person. It's essentially a smart camera "guessing" your age, much like a human might estimate someone's age by looking at them, but trained on millions of faces for greater accuracy. Companies that have developed such models include Yoti and FaceTec. This method addresses many privacy concerns: it is anonymous age-checking. In the words of an FTC filing, "facial age estimation . . . without facial recognition . . . cannot work out anything other than the person's estimated age."[360] In other words, the system is not identifying you, just your approximate age, and it is usually configured to report a simple yes/no (e.g., "age over 13 confirmed").[361]

243. This technology was feasible years ago and has been used successfully in a number of settings. By 2018, Yoti's AI had reached a level of accuracy that attracted government trials. The UK Home Office ran tests in 2019–2020 using Yoti's age estimation at supermarket self-checkouts to verify age for alcohol purchases; it reported that "no underage customers purchased age-restricted items when using the system," and noted public "appetite for digital age assessment."[362] By 2020, Yoti's AI system was estimated to be 98.9% reliable at classifying adults vs. minors within a small margin of error.[363] In 2022, the French data regulator (CNIL) analyzed age verification methods and concluded that using facial analysis via a device's camera (with no

[360] April Tabor, Application for Approval of a Veritable Parental Consent Method Pursuant to The Children's Online Privacy Protection Rule 16 CFR Section 312.12(A) at 4.

[361] *Id.*

[362] UK government completes trials of age estimation technology, Computer Weekly, (January 12, 2023) https://www.computerweekly.com/news/252529133/UK-government-completes-trials-of-age-estimation-technology.

[363] This AI Predicts How Old Children Are. Can It Keep Them Safe?, Wired (October 26, 2021) https://www.wired.com/story/ai-predicts-how-old-children-are/.

biometric identification) is an acceptable and effective solution for keeping minors out of adult sites.[364] In practice, this means the system should analyze the face locally or on a secured server, output an age result, and not retain the image – a design now standard in products like Yoti.

244. In 2022, Instagram rolled out a facial age estimation feature (powered by Yoti) in multiple countries, including the U.S. and UK, to verify users who changed their date of birth from under 18 to over 18.[365] A user attempting to say "I'm an adult" after previously stating they were younger can be asked to upload a quick video selfie. The AI then estimates their age to confirm if they are indeed over the threshold.[366] Critically, however, as explained in the previous section, Instagram does not require this method of age verification in the first instance, making it easy for underage kids to circumvent it.

245. **Pros:** Extremely low friction – all the user does is look into a camera for a couple of seconds. No forms to fill, no documents to provide. It is instant (results in seconds) and scalable to millions of checks per day. It can also be made privacy-preserving (no personal info retained). It is also affordable at scale.[367]

246. **Cons:** It's not 100% perfect; an AI could misclassify some borderline cases (*e.g.*, a 12-year-old might look 13, or a youthful 19-year-old might look 17). However, for broad safety-gating, it can be tuned to be conservative – for example, Instagram/Yoti claim very high accuracy in detecting users under 13, often erring on the side of labeling teens as pre-teens rather than missing a child. Another consideration is fairness and avoiding bias – these systems need to be trained on diverse faces. However, existing systems have been effective in this area. Yoti has published white papers and obtained independent audits (*e.g.*, by the UK's Age Check Certification Scheme) verifying that its accuracy is consistently high across different ethnicities and genders.[368] The fact that regulators and standards bodies have begun certifying these AI age checks speaks to their maturity.

247. In sum, facial recognition technology was feasible by 2018. By that time any company serious about keeping under-13 users out (or providing age-appropriate experiences) could

---

[364] Online age verification: balancing privacy and the protection of minors, CNIL, (September 22, 2022) https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

[365] Introducing New Ways to Verify Age on Instagram, (June 23, 2022) https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram.

[366] Instagram's parent company Meta has likewise started using this for Facebook Dating to ensure minors (under 18) cannot access that service. META3047MDL-020-00705117.

[367] META3047MDL-065-00041181 (indicating Yoti charged Meta $750,000 a year for 433,000 "API calls").

[368] Facial Age Estimation White Paper, Yoti, (September 9, 2024) https://www.yoti.com/blog/yoti-age-estimation-white-paper/.

leverage facial age estimation AI as a seamless checkpoint. The cost per check is modest – typically a small fee to the provider (much less than a dollar, especially at volume) or just computational cost if done in-house. Given that this method requires no personal data retention, it squarely addresses the excuse that "privacy concerns" made age verification impossible. The technology ignores identity and only assesses age, acting like a privacy-conscious bouncer at the door.

B. Negligible Costs Compared to Massive Revenues

248. Beyond technical feasibility, an important question is cost. Tech companies may argue that instituting rigorous age verification would be prohibitively expensive. The evidence shows the opposite: the cost of deploying these measures at scale is small, particularly relative to the Defendants' revenues. In many cases, the cost is effectively zero for the platform (the user bears a small verification fee, or a third party handles it for pennies). Even where the platform might pay a service fee, it's on the order of cents per user.

249. To put this in perspective, consider a credit card verification. As discussed, Nintendo and others charged $0.50; Google charges $0.30 for a parent verification on Family Link (to cover the payment processor fee) and then immediately refunds it.[369] In other words, Google spends a few dimes per new child user to ensure a parent is involved – and it still offers the Family Link service "completely free." For a social platform, even if performing millions of verifications, this would only amount to a few million dollars in one-time processing costs. As noted above, Meta (Facebook/Instagram) had revenues of roughly $117 billion in 2022. Even if verifying every single one of its ~3 billion users with a $0.50 transaction were needed, that would be $1.5 billion – about 1.3% of one year's revenue. In reality, the percentage would be far smaller, because not all users need credit card verification, and cheaper methods like AI age scans could be used for the majority.

250. Third-party verification services like IDWise advertise enterprise pricing of about $1 per verification for robust ID checks. Volume discounts and simpler checks (like just age, not full identity) could drive this much lower. AI age estimation is even cheaper.

251. In summary, the direct costs of implementing real age checks is economically feasible for even the largest user bases. The costs per user range from a few cents to a few dollars at most, and those are one-time costs, not recurring. Against the backdrop of multi-billion-dollar revenues, this is a drop in the bucket.

[369] Why Am I Prompted to Enter a Credit Card to Create a Nintendo Account for My Child?, https://en-americas-support.nintendo.com/app/answers/detail/a_id/1334/~/why-am-i-prompted-to-enter-a-credit-card-to-create-a-nintendo-account-for-my; https://www.lifewire.com/how-to-use-google-family-link-4174557.

252. The true cost to these platforms is the potential loss of revenue they earn from advertising to the millions of young children's accounts on their platforms.[370] Unlike direct costs of verification, the loss of that revenue could significantly impact the companies' bottom lines. That, however, does not justify the unlawful and irresponsible targeting of young children with platforms known to be harmful to them.

C. Early Adopters: Age Verification in Gaming and Mobile Device Platforms

253. One of the strongest responses to the notion that "robust age verification wasn't possible" is the fact that related industries already did it. From video game consoles to mobile operating systems, there are real-world case studies showing these methods in action – in some cases deployed by the same tech giants who failed to use them on their social media platforms. The following are some examples:

1. Video Games and Consoles – A Decade of Parental Gates

254. The gaming industry had to confront online child safety early, largely due to COPPA and the presence of voice/chat features in games. Microsoft, Nintendo, and Sony each implemented parental consent and age gates as they expanded their online services. Already mentioned above is Nintendo's $0.50 verification fee for child accounts on the Wii U in 2012. That system was straightforward and effective – no child under 13 could create an account without a parent's involvement. Once the parent unlocked the first account with a credit card, additional child profiles could be managed with a PIN (recognizing that the adult had been verified already).

255. Microsoft's Xbox Live similarly required that children (under 13) be added to an adult's Microsoft Account family. As far back as the Xbox 360 era (late 2000s), Microsoft distinguished between "child accounts" and "parent accounts." If a child tried to sign up, the system would prompt for an adult to sign in and approve. By 2012, Microsoft had an online mechanism where the adult would verify via a small credit card charge to confirm they were 18+.[371] In June 2023, the FTC settled a case with Microsoft for failing in some aspects of COPPA compliance on Xbox (allowing child accounts to proceed too far in registration without parental notice), which Microsoft is now remedying with even stronger safeguards.[372] Microsoft's remedial commitments

[370] *See, e.g.*, Social Media Platforms Generate Billions in Annual Ad Revenue From U.S. Youth, Harvard School of Public Health, (December 27, 2023) https://hsph.harvard.edu/news/social-media-platforms-generate-billions-in-annual-ad-revenue-from-u-s-youth/.

[371] *See, e.g.*, Networking Your Xbox, Informit, (May 3, 2012) https://www.informit.com/articles/article.aspx?p=1834696&seqNum=2.

[372] FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent, FTC, (June 5, 2023)

include obtaining parental consent for any account that indicates a child age and deleting data if consent isn't obtained.[373]

256. Sony's PlayStation Network (PSN) also utilized age verification. Initially, PSN had a "master account/sub-account" system where sub-accounts for under-18 users had limitations. In 2017, Sony revamped to a "Family on PSN" system. As part of that change, they introduced a one-time $0.50 charge for North American users setting up an adult account (which by extension verifies the person acting as family manager is adult).[374] This covers the scenario where a teen or child might try to falsely set up as an adult; the card check prevents that. On the child side, creating a sub-account for someone under 13 requires going through the family manager's account, which by then is verified.

2. Mobile Operating Systems and App Stores – Built-in Age Gating

257. Both Apple's iOS and Google's Android introduced comprehensive family account systems in the mid-2010s that baked in age verification and parental consent. Apple's Family Sharing (launched in iOS 8 around 2014) allowed an organizer to create an Apple ID for a child. Apple explicitly required that the organizer be an adult with a verified payment method.[375] This means Apple knows the age of the child and can restrict certain content (for instance, a 12-year-old's account cannot download 17+ rated apps without the parent's consent). The App Store also can enforce age ratings because it knows the user's birth date from the account creation. All of this flows from that initial age verification step. Apple's approach demonstrates how age assurance can be integrated elegantly into the user experience. Millions of families use it. Apple improved methods recently: in iOS 16, they added the ability to use a digital ID in Apple Wallet to verify age.[376] This further reduces friction while keeping the age gating requirement intact.

258. On the Android/Google side, Family Link (officially launched 2017 after a pilot) allowed creation of Google Accounts for kids under 13, managed by the parent. The signup flow forces the parent to authenticate and then verify with a small credit card charge (typically $0.30 in the

https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information.

[373] *Id.*

[374] PS4's 5.0 Update Revealed, Here's What It Does, Gamespot, (August 18, 2017) https://www.gamespot.com/articles/ps4s-50-update-revealed-heres-what-it-does/1100-6452596/.

[375] Create an Apple Account for Your Child, https://support.apple.com/en-us/102617.

[376] This is mentioned in their support: you may use a driver's license in Wallet where available instead of a credit card. *See* https://support.apple.com/en-us/111803.

U.S.).[377] Google explains this is required to comply with COPPA. After that, the child's account is marked as under 13 and has various protections (no targeted ads, SafeSearch on, Play Store restrictions, etc.). Notably, while Google uses this technology on its Android platform, it does not use it on YouTube (a platform it also owns). Instead, as noted above, individuals in the U.S. can sign up for YouTube and access all content without any age verification (beyond providing a birthdate).

259. Notably, this is not true in other countries. In 2021, YouTube began requiring the upload of an ID or credit card for age verification on certain content in Europe.[378] This was to comply with the EU Audiovisual Media Services Directive (AVMSD) which mandated stricter age checks for adult content. So if a user in, say, Germany attempts to view a restricted video and YouTube isn't sure they're 18 (perhaps their account has no birthday or shows them as under 18), YouTube will now prompt: "Verify your age by providing ID or credit card." This shows that Google can impose such checkpoints even on legacy accounts when regulation compels it.

260. In summary, mobile platform operators have for more than a decade treated age verification as a standard feature. They leveraged the same techniques available to everyone: credit cards, IDs, and trusted login flows. The fact that Apple and Google – two of the world's largest tech companies – implemented these measures demonstrates that these systems could have been deployed at scale by the Defendants, who are similarly large and technologically sophisticated. Unlike the Defendants, mobile platform operators prioritized building frameworks to differentiate adults and children and enforce appropriate policies. Social media platforms could have, and should have, done the same.

D. Conclusion

261. For over a decade, the social media industry's approach to age verification was a textbook example of too little, too late – and in truth, often nothing at all. The Defendants built digital playgrounds and invited the world, put up a token age limit sign, and then shrugged as elementary and middle-school children flooded in. It was a broken system that put the onus on kids to self-regulate and on parents to play catch-up, while the platforms themselves sat back and watched their user numbers climb.

262. While the Defendants denied or downplayed what was happening on their platforms, internal records indicate a gap between their public stance ("we don't allow under-13s, problem solved") and private reality ("millions of kids are here and driving our metrics"). This is most

[377] Access Age-Restricted Content and Features https://support.google.com/accounts/answer/10071085.

[378] Watch Age-Restricted Videos, https://support.google.com/youtube/answer/10070779.

troubling because it may lull regulators and parents into a false confidence that the issue is being handled.

263. By reviewing the timeline and evidence, it becomes apparent that by 2010, the existence of effective parental consent systems was widely known and their efficacy demonstrated. This set an industry standard: a reasonable company in the online services space that knows it has children on its platform should implement verifiable parental consent and age gating as other responsible companies have.

264. Social media companies failed to adopt these reasonable measures. They had ample examples to emulate – whether by integrating a credit card verification on sign-up, implementing a parent-managed sub-account system, or partnering with app stores to enforce parental approval (as Meta belatedly suggested in 2023) – but did not follow them.

IX. OPINION 4: PARENTAL CONTROLS WERE MISSING, WEAK, AND/OR OPT-IN

265. For most of the 2010–2022 period, the Defendants' social media platforms offered parents and guardians virtually no effective tools to supervise their children's online activity. When parental control features eventually arrived – often belatedly, or after public pressure or regulatory sanctions – they were weak, optional add-ons. Critically, these tools required the child's cooperation to activate and could be easily bypassed. Even when enabled, they gave parents and guardians only a narrow, blurred view of what their kids were actually doing or seeing online. In short, Defendants' parental control designs were underdeveloped, opt-in by design, and riddled with loopholes, falling well below the standards utilized in other technology sectors.

A. Years of Delay: Parental Controls Arrived a Decade Late

266. By the time the Defendants implemented meaningful parental supervision features in the early 2020s, millions of minors had already been active on their platforms for years with no parental or guardian oversight. These changes were introduced following a series of whistleblower revelations, congressional hearings and FTC fines. A brief timeline highlights how late and reactive these efforts were:

267. **Instagram/Facebook (Meta):** In 2009, Mr. Zuckerberg was sent an email by another Meta executive, Jeff Rothschild, entitled "Let parents be parents on Facebook."[379] In this email, Mr. Rothschild advised Mr. Zuckerberg that Facebook should "add an opt-in feature, which would allow a Facebook user (child) to designate another user (the parent) to have certain auditing rights

[379] META3047MDL-040-00225130.

and limited controls over the child account."[380] Mr. Rothschild advised that, in his view, this was "the only scalable and effective way to address the issue of minors on Facebook"—"[t]he dynamic that this creates is to give parents an opportunity to act as parents on Facebook as they would in other dimensions of their children's lives." Two years later, Meta's former Product Leader for Site Integrity, Arturo Bejar, began advocating for Meta to adopt parental controls.[381] According to Mr. Bejar, Meta "was thinking about having kids under 13 on the platform" and how to "design parental supervision so that [it] helps parents and kids to be safe online."[382]

268. Despite these early internal discussions, Meta waited until 2022 – more than 13 years after Mr. Rothschild's email – to implement parental controls on Instagram.[383] And it waited until 2023 to implement parental controls on Facebook.[384] Mr. Bejar acknowledges that "Meta had the engineering capacity to build a parental supervision tool" in 2011, but testified that it "was not a priority."[385] Meta's roll-out of "Family Center" tools came only after intense public scrutiny in late 2021 over Instagram's harms to teens (following whistleblower revelations).

269. **Snapchat (Snap):** For the first 11 years of Snapchat's existence (2011–2022), the platform offered no parental controls at all. Snapchat finally released its "Family Center" feature in August 2022, on the heels of congressional hearings regarding Snap's management of children on its platform.[386]

270. **YouTube (Google):** The main YouTube platform similarly lacked any parent-supervised account system for teens until 2021, when Google introduced "Supervised Experience" accounts, allowing parents to link to a teen's YouTube account in a limited way.[387] This program was announced more than 15 years after YouTube's launch. Prior to that, Google offered a separate YouTube Kids app for children under 13, but provided no parental oversight options for teens on

[380] *Id.*

[381] Bejar Dep. at 579:19-25.

[382] Bejar Dep. at 579:25-580:9.

[383] Introducing Family Center and Parental Supervision Tolls on Instagram and in VR, Meta, (March 16, 2022), https://about.fb.com/news/2022/03/parental-supervision-tools-instagram-vr/.

[384] Bejar Dep. at 579:7-18.

[385] Bejar Dep. at 580:14-581:1.

[386] Introducing Family Center on Snapchat, (August 9, 2022), https://values.snap.com/news/introducing-family-center-on-snapchat; S. Hrg. 117-843 — PROTECTING KIDS ONLINE: SNAPCHAT, TIKTOK, AND YOUTUBE https://www.congress.gov/event/117th-congress/senate-event/330808.

[387] A New Choice for Parents of Tweens and teens on YouTube, https://blog.youtube/news-and-events/supervised-experiences-for-families-on-youtube/.

the main YouTube platform. This change came on the heels of a $170 million FTC fine against YouTube in 2019 for children's privacy violations.

271. **TikTok (ByteDance):** Prior to 2020, TikTok had no parent supervision features, despite its immense popularity with middle-school and high-school users.[388] TikTok introduced its "Family Pairing" parental control mode in 2020, shortly after the FTC fined it $5.7 million for violating child privacy laws.[389]

272. In each case, the deployment of parental controls on these social platforms was delayed by years compared to both the needs of their user base and the norms of other industries (which are described in Opinion 5 of my report).

B. "Opt-In" Oversight Requiring Teen Cooperation (Safety Not Enabled by Default)

273. When the Defendants finally did add parental supervision features, they designed them in ways that were predictably ineffective. For example, rather than making parental controls a default for children's accounts, they were made "opt-in," meaning that the user would have to navigate a complicated set-up process to activate it.[390]

274. To set up Family Center on Snapchat, parents or guardians must download the application, set up a Snapchat account of their own, add their teen as a "friend," send their teen an invite to join Family Center, and wait for their teen to accept the invite.[391] Similarly, when Instagram's supervision tool was introduced in 2022, the parent had to set up an account, and then the teen had to send an invite to the parent to link the two accounts.[392] TikTok's Family Pairing involves scanning a QR code on the teen's phone or sending an invite to link accounts.[393] The Defendants made these features opt-in even though their documents and testimony showed that "[i]f a feature

[388] TIKTOK3047MDL-001-00000204; TIKTOK3047MDL-022-00522755.

[389] TikTok Hit with Record Fine for Collecting Data on Children, CNN, (February 28, 2019) https://www.cnn.com/2019/02/28/tech/tiktok-ftc-fine-children.

[390] Bejar Dep. at 581:17-582:1.

[391] How do I Add My Teen to Family Center, https://help.snapchat.com/hc/en-us/articles/8132784476820-How-do-I-add-my-teen-to-Family-Center.

[392] Later, this was modified so that a parent could send the invite, with the teen approving it.

[393] Family Pairing https://support.tiktok.com/en/safety-hc/account-and-user-safety/family-pairing#2; TIKTOK3047MDL-111-LARK-05818491 at -492.

is opt-in, almost nobody will use it,"[394] and that "teenagers . . . don't go into settings."[395] This fundamentally undermined their effectiveness – the vast majority of teens never enabled these features, and thus remained unsupervised by default. A former Meta executive described the situation as follows: "the dirty secret about parental controls is that the vast majority of parents don't use them . . . unless the defaults are set to restrictive settings, which most are not, they do little to protect users."[396]

275. Empirical evidence bears this out. Meta reports that [redacted] of Youth users predicted to reside in the U.S. . . . were enrolled in Supervision through Family Center on Instagram between March 23, 2025 and March 24, 2025."[397] Similarly, for TikTok, as of 2023, only 0.25% of US users enabled Family Pairing and only 1% of users 13–16 had Family Paring enabled.[398] TikTok found internally that this was a direct effect of the complicated set-up process involving a QR code, noting that "[a]round a million potential users a week will enter Family Pairing each week and when they reach the QR screen over 90% of them drop," that "the QR code we use to currently facilitate pairing is very inconvenient. [P]arents who discover FP cannot take action to invite their teens to link. [I]nstead they have to wait until they are together with their teen and initiate linking in person."[399] Another TikTok engineer acknowledged that "Family Pairing is where all good

[394] Bejar Dep. at 167:15-24; *see also* TIKTOK3047MDL-098-04111887 at -898 (noting that "**anything opt in gets very low usage**").

[395] Bejar Dep. at 548:16-22; *see also* id. at 582:3-10 (Q. "What impact would those features of parental supervision have for adoption and effectiveness based on your industry experience?" A. "It would mean that the feature would not be adopted and then as such would not be effective as a safety feature.").

[396] Meta Says Parental Controls Protect Kids But Hardly Anyone Uses Them, Washington Post, (January 30, 2024) https://www.washingtonpost.com/technology/2024/01/30/parental-controls-tiktok-instagram-use/.

[397] Meta's Sixth Supp. Response to Interrogatory 12.

[398] Han Ex. 22; Han Transcript 191:24-192:8; TIKTOK3047MDL-004-00138339. Family Pairing was also sloppily designed, sometimes resulting in parents who did use it unintentionally creating a less safe experience for their child. For example, when a parent first enabled Family Pairing, the child's privacy settings would reset to default, even if the child had previous enabled more protective settings, and TikTok did not notify teens or parents that their privacy settings were overridden. TIKTOK3047MDL-079-LARK-02280126. Family pairing would also cause a child's daily screen time limit to be disabled. TIKTOK3047MDL-084-LARK-03148936. These errors led the product manager in charge of Family Pairing at TikTok to joke "Haha Family Pairing is where all good product design goes to die it seems. It makes some sense though, it really hasn't been anyone's priority outside of urgent action in response to regulators."

[399] TIKTOK3047MDL-067-LARK-01027037.

product design goes to die . . . [I]t really hasn't been anyone's priority outside of urgent action in response to regulators."[400]

276. YouTube's parental supervision is piecemeal and not easy to use. Family Link, for example is not a specific parental control and requires configuration from a completely separate settings area- which is different depending on device type.[401] Further, 65% of the population does not have the opportunity to set this up as it only applied to Android and Chromebook.[402]

277. Because parents and guardians cannot access Snap's Family Center without their child's approval,[403] the feature is optional and easily bypassed by minors who do not grant their parents or guardians access or by creating multiple accounts.[404] Only 27% of Snap Family Center invites are accepted.[405]

278. Internal documents show that Snap was aware Family Center had an extremely low adoption rate.[406] In April 2024, Mr. Speigel, Snap's CEO, testified in front of the U.S. Senate Judiciary Committee that of the approximately 20 million teenage Snap users, only about "200,000 parents use Family Center and about 400,000 teens have linked their account to their parents using Family Center."[407] In other words, only about 2% of minor-used accounts are linked to and monitored for safety via "Family Center."

279. Internal documents further show that Snap did not effectively promote adoption of Family Center with their minor users.[408] Instead, Snap made Family Center **"extremely hard to find in the app,"** *especially* for parents or guardians who themselves were not users of the app and therefore less familiar with navigating the platform – which Snap hypothesized is exactly the case for most parents of 13 to 17 year olds.[409]

280. For some of these platforms, teens not only had to consent to parental controls in the first instance, they retained the power to disable or evade the supervision thereafter. For example, TikTok's Family Pairing can be turned off by the teen at any time in the app settings; when a teen

[400] TIKTOK3047MDL-036-LARK-00164712 at -713.

[401] GOOG-3047MDL-03721198 at -210, GOOG-3047MDL-05630293.ECM at -294.

[402] GOOG-3047MDL-05214601 at -601.

[403] https://help.snapchat.com/hc/en-us/articles/8132840494996-Why-can-t-I-see-my-teen-s-account-in-Family-Center.

[404] SNAP2071682.

[405] SNAP4350328 at -341.

[406] SNAP0002545; SNAP1282068; SNAP1186211.

[407] SNAP1282068 at 139.

[408] SNAP1837695.

[409]SNAP0019076 at -078-079.

unlinks from Family Pairing, the parent or guardian gets a notification sent through the TikTok app, but the teen's account immediately returns to an unsupervised state unless the parent can persuade them to re-link. "If a parent does not frequently check the TikTok app every 48 hours, the teen can unlink and use TikTok without restrictions without the parent being aware."[410] TikTok recognized "the ease with which teens can turn it off, even over parental objection, largely renders the family pairing function useless."[411] TikTok considered but rejected a proposal to require parental approval to unlink accounts.[412]

281. Snapchat's Family Center similarly allows either the parent/guardian or the teen to "leave Family Center at any time," which will break the link – the app will notify the other party, but cannot prevent the teen from removing themselves. In other words, a teenager who feels constrained can one-sidedly opt back out of supervision. This fundamentally differs from, say, parent controls on a gaming console or phone, where a child cannot simply turn off the restrictions without the parent's or guardian's passcode.

C. Minimal Visibility: Parental Tools that Reveal Little About Activity

282. Even in the minority of cases where families do enable these supervision features, the scope of parental insight is extremely limited. Defendants' parental control tools have been appropriately criticized as providing only a surface-level view – showing parents or guardians a few high-level indicators, but not the substance of what their child is doing or encountering on the platform.

283. Specifically, the major platforms' tools do not allow parents or guardians to see or monitor what the platforms recommend, promote, and push to their children. Instagram's supervision features allow a parent or guardian to view the accounts their teen follows and get notified if the teen reports another user, but parents or guardian cannot view the actual photos/videos or recommended content appearing in the teen's feed. As noted previously in Section VI(c)(4), TikTok's Family Pairing gives parents and guardians the ability to set some content filters (*e.g.*, enabling a restricted mode to limit mature content) and disable direct messages to the teen, but it does not show parents or guardians which videos the platform is presenting to the teen, let alone explain why it is choosing those for recommendation.[413] (It also was found by TikTok's own

[410] Furlong Dep. Ex. 100.

[411] TIKTOK3047MDL-004-00138339 at -341; Furlong Dep. 97.

[412] Furlong Dep. Ex.98; Furlong Dep.. at 635:23-636:3.

[413] TikTok was aware that Restricted Mode was "not in line with stakeholder expectations", but did not inform users and parents of that fact. Ulucay Ex. 23; Deposition of Amy Ulucay (February 5, 2025) at 224:22-225:9. TIKTOK3047MDL-015-00338864 at -865 ("Restricted Mode does not meet user expectations [in] almost all content themes (violence, gore, profanity, adult, etc.)"); TIKTOK3047MDL-036-LARK-00111985 at -986 ("[C]urrent restricted mode lacks sufficient feed safety standards, posing high risks to users"); TikTok was also aware that at,

engineers to be ineffective at filtering age-inappropriate content).[414] In essence, none of these "parental control" modes permit a parent to observe or identify potentially harmful activities on the platforms.

284. Key aspects typically hidden from parents under these systems include:

- Feed Content and Recommendations: Parents and guardians cannot see what posts or videos the child is viewing in their feed or "For You" page, nor what the algorithm is actively recommending to that child. This is critical because harmful content (*e.g.*, self-harm or pro-eating-disorder posts) often is pushed via algorithmic recommendations unknown to parents.

- Live or Ephemeral Content: Content that appears briefly (stories, live streams, or snaps) is effectively invisible to parents and guardians. For instance, if a teen views a toxic live stream on TikTok or an inappropriate Snapchat Story, parental supervision won't retrospectively surface that.

- Search and Browsing History: Unlike some web filters that let parents or guardians review a child's search queries, social media supervision tools do not show what topics or hashtags a teen has searched for. A teen could be searching for dangerous challenges or illicit content and the parent would be none the wiser through the official tools.

285. These particular supervision features may be unnecessary for certain families, and their utility and need will doubtless depend on the age and maturity of the child and the particular circumstances of any given family. With that said, parents should rightly expect access to these options, rather than social media being an "all or nothing" proposition for families.

286. In short, the granularity of monitoring is extremely low. The typical information a parent might get is: how much time the teen spent on the app, a list of the teen's friends or followers, and perhaps notification of new friends/follows or if the teen reports someone. These are useful but very high-level signals. They do not tell a parent or guardian if their child is being groomed by a stranger, bullied by peers, exposed to self-harm content, or any number of other dangers that occur on the platforms.

D. "Finsta" Accounts and Other Loopholes Allow Teens Evade Supervision

287. Beyond the limitations described above, teens are also able to easily circumvent these tools by creating secondary accounts that their parents or guardians do not know about. On Instagram, for example, it is routine for teens to maintain a "finsta" ("fake Insta") – a private account shared

---

at one point, it was "showing unsafe [search] results for people using Family Paring compared to under 18 [users] registered without it." de Bailliencourt Ex. 42.

[414] *See* Section VI(c)(4) (discussing the company's findings).

only with friends – in addition to their main account that parents might be aware of. A parent might diligently supervise one account, while the teen does as they please on the other.

288. None of the platforms' parental tools detect or prevent this. Instagram, Snapchat, TikTok and YouTube do not, for example, alert a parent or guardian if their child's device spins up a new account or if the child has multiple accounts. Moreover, as the platforms lack age verifications, parental consent and default parental controls, there is nothing to stop a teen from creating a new account without a parent's or guardian's knowledge.

289. Internal documents produced in this litigation show the Defendants were aware of this behavior, and, in some instances, encouraged it. For example, internal Meta documents discuss Meta's "Finsta Growth" program, "an effort on the Growth team to encourage teens to create their first Finsta account and to teach them to use the multi-account switcher."[415] In explaining the rationale for this program, the document notes that "on finstas, teens post 3x as much content."[416] Other Meta documents highlight that teens may be "connect[ing] with the wrong people (parents)," which could decrease engagement, and note that "[o]ne advantage of these secondary accounts are getting away from parents or relatives who are following teens' public accounts."[417]

290. TikTok similarly discussed that there were about "2,500 daily account switching and log out actions" at day, which would allow teens to "switch to a different account that was not linked to their parents."[418]

291. Snap's internal documents show children are motivated to create multiple Snap accounts in order to avoid parental control.[419] Snap conducted a survey of users aged 13-17 and found "the primary reason for having multiple accounts on Snapchat is to separate and manage different audiences (*e.g.*, parents, teachers)."[420] According to Snap's Activation Team's internal research, 46% of power users aged 13 to 17 have multiple Snap accounts. This is unsurprising considering Snap's account creation process requires no verifiable information.[421] Also, because Snap does not notify parents/guardians or require parental consent, minor users are able to create multiple Snap accounts without parents or guardians knowing.

292. The net effect is that the platforms' parental controls can be rendered ineffective with a few simple actions by a minor, without the parents' knowledge.

---

[415] META3047MDL-031-00086273 at -274.

[416] *Id.* at -275.

[417] META3047MDL-031-00088636 at -636.

[418] Furlong Dep. 643:4-644:1, Exhibit 100.

[419] Chan Dep. Ex. 21; Chan Dep. Ex. 24.

[420] SNAP3118038 at -070.

[421] Chan Dep. at 393:25-395:14.

E. Misstatements Gave Children, Parents, Guardians and the Public a False Sense of Security

293. The Defendants made other misleading statements that strongly suggested to children, parents, guardians and the public that their platforms were safer than they actually are.

294. For example, Instagram's website stated, "We do not allow nudity on Instagram."[422] It further states that the "prevalence" of "adult nudity and sexual activity violations" is just "0.02% to 0.03%."[423] As Mr. Bejar noted during his deposition, this creates "the impression that you're not going to get that kind of content recommended to you on Instagram" – "I look at this as a parent and somebody who has worked in the field and I think, oh, yea, it's very unlikely that my kids are going to be getting any of that stuff."[424]

295. However, what Meta does not disclose to parents is that, in its own internal studies, 19% of children aged 13 to 15 reported seeing unwanted nudity or sexual images on Instagram in the last seven days.[425] In fact, Mr. Bejar set up a new account as a 13-year-old. Watching only Reels served by the Instagram algorithm, it took just "8 to 12 minutes" to get to the point where the account "was getting back-to-back sexual Reels recommended to that account."[426] This included, for example, videos of adults masturbating.[427] Mr. Bejar conducted similar experiments with suicide and self-harm and found that such content was widely available to children and was not taken down when reported.[428] Meta did not provide teens, parents or guardians with any warning that they would be exposed to this type of material.[429] Instead, as Mr. Mosseri admitted, this information "like every other survey we run, is not provided to the public."[430]

296. Meta's internal research and studies showed that other harms to children were prevalent on the platform as well, including bullying, hate speech, encouragement of suicide and self-harm, encouragement of eating disorders, sale of drugs and sexual services, sextortion, revenge porn,

---

[422] Bejar Dep. at 209:23-25.

[423] Bejar Dep. Ex. 25; Mosseri Dep. at 482:21-486:23.

[424] Bejar Dep. at 336:17-25; Mosseri Dep. at 486:14-20 ("This is the overall percentage of times that people saw anything … of all the times someone saw anything, what percentage of those times was the content violating our adult nudity and sexual activity guidelines").

[425] Bejar Dep. at 333:15-334:1, 336:5-10.

[426] Bejar Dep. at 217:12-218:9; *see also id.* at 219:12-221:1 (describing methodology).

[427] Bejar Dep. at 222:6-24.

[428] Bejar Dep. at 403-405.

[429] Bejar Dep. at 221:3-15.

[430] Mosseri Dep. at 514:20-23.

unwanted sexual advances by adults, and more.[431] Meta did not disclose these findings to the public, or otherwise warn about the harms to children that the studies identified.[432]

297. The disclosures also ignore the prevalence of Instagram direct messages, or "DMs." Meta knew at least in 2018 that DMs are "where all of the bad stuff happens."[433] Meta's only filter for DMs was for "known instances of child exploitative imagery" until 2024, when Instagram added a "nudity" filter for DMs.[434] "Known instances of child exploitative imagery" would not stop, for instance, an adult sending a "dick pic" to a minor.[435] Nothing on Instagram's "Transparency Center" explained or implied this vulnerability until the nudity filter's roll-out in 2024.[436]

298. Rather than publish the results of its research, Meta hid it, including from its own employees. For example, the largest and most comprehensive study – the BEEF study – was "locked down," meaning the vast majority of Meta employees had no access to it and no awareness of it.[437] This was an unusual departure from Meta's typical policy, which allowed employees to view and make use of research from other teams.[438] Meta went further and deleted key portions of the data from the BEEF study before it could be analyzed by Meta's researchers.[439]

299. For the public, Meta put out misleading "prevalence numbers" that minimized the risks they had identified, and "mislead parents and, you know, the rest of the world as to what is the actual unfolding of harm on Instagram."[440]

---

[431] *See* Bejar Dep. at 119:11-13, 122:17-125:24 (discussing results of "NES" survey); *id.* at 365:5-401:25 (discussing results of 2021 "BEEF" study); *Id.* at 346:21-347:1 (It was "well known among the well-being team at Meta and others that suicide and self-injury and self-harm content was easily accessed on Instagram by kids.").

[432] Bejar Dep. at 271:7-14, 305:15-306:1, 331:22-332:2, 405:25-406:8, 489:23-480:3.

[433] META3047MDL-040-00215891.

[434] Mosseri Dep. at 233:12-239:19.

[435] *Id.*

[436] *Id.*; *see also id.* at 486:24-487:2 ("**Q.** Okay. The information on here doesn't contain Direct Messaging content? **A.** For this specific metric, I don't believe so. I'm not sure.").

[437] Bejar Dep. at 491:16-492:15, 500:25-501:7.

[438] *Id.*

[439] META3047MDL-034-00504889 at -889 ("BEEF asked a question about emotional impact, but I was told I need to delete that data/ we can't analyze it . . . . We're not allowed to ask about emotions in surveys anymore").

[440] Bejar Dep. at 332:3-9; *see also id.* at 204 ("[T]his Transparency Center was deeply misleading as to what is the likelihood that your kid is going to experience a certain harm."); 340:15-25, 365:16-366:24 (bullying); 341:14-342:23, 368:10-369:21 (child endangerment); 205:4-19, 370:10-371:3, 401:4-402:1, 421:3-422:9 (suicide and self-injury).

300. More recently, Meta has attempted to alter the design of its studies in order to downplay the platforms' harms. For example, in a discussion of a 2024 study known internally as "MYST," employees internally raised concerns that the study was unlikely to "advance the narrative that Meta wants"; in particular, "**MYST is likely to find negative associations between teen mental health and social media**."[441] The document recommends "modify[ing]" the study to advance certain "external goals," including: "Deflat[ing] conversations about research claiming causal connections between social media and mental health and well-being. . . . ." and "Advanc[ing] the credibility of research that finds small or null correlations between social media [and] well-being."[442] In other words, Meta proposed *changing the study* so that it would undermine, rather than support, claims that social media is harmful.

F. Conclusion

Defendants' handling of parental controls reveals a pattern of systematic underdevelopment and design neglect. The Defendants' social media platforms failed to provide parents with effective supervision tools at all from 2010 through the early 2020s. When they finally introduced parental controls, they were designed as "opt-in" features, rather than defaults, ensuring that they would not be widely used. They were, moreover, riddled with loopholes that allowed tech-savvy (or even not-so-savvy) teens to sidestep monitoring entirely through, for example, secondary accounts.

X. OPINION 5: BETTER PARENTAL CONTROLS WERE STANDARD PRACTICE ELSEWHERE

301. In other corners of the tech industry, companies erected strong parental controls years before social media's rise. Video game consoles, streaming services, and educational platforms all implemented robust, parent-linked controls well before social media hit its user boom. These systems – mandatory child accounts linked to parents, time limits, activity reports – were not cutting-edge experiments but widely deployed, mature technologies. They earned praise from regulators and safety experts as responsible practices. In glaring contrast, the major social media platforms lagged far behind these standards. As a result, harms that were minimized on well-fenced platforms proliferated unchecked on social media.

[441] META3047MDL-072-00317597 at -599.

[442] *Id.* at 597-99.

A. A Timeline of Parental Control Leadership in Other Industries

302. Years before social media dominated youth online activity, other industries had already embraced parental controls as standard operating procedure. A brief timeline highlights how early and widespread these safety fences became:

303. **Mid-2000s (Video Games – Content Filters):** By 2005–2006, console makers baked in parental controls at launch. The Xbox 360 (launched 2005) and PlayStation 3 (2006) both included settings to restrict games by age-rating (the ESRB system). This meant a parent could block mature-rated games entirely on day one. These were not optional add-ons but core features of the platforms.

304. **Late 2000s (Video Games – Playtime Limits & Accounts):** Console makers soon went further. In 2007, Microsoft rolled out the "Family Timer" on Xbox 360, letting parents set daily or weekly time limits on console use.[443] When time ran out, the system would automatically shut off the game. Microsoft even partnered with the National PTA to educate parents on using these tools.[444] By this time, as noted above, consoles also required child accounts to be created under parent accounts for online services.

305. **Early 2010s (Video Games – Refinement and Monitoring):** The early 2010s saw these controls expand in sophistication. By 2011, Nintendo's online network and later the Nintendo Switch (2017) offered a dedicated parental control smartphone app for monitoring play.[445] With this, parents could see what games were played and for how long, get monthly activity reports, and adjust controls from their phone. They could set daily play-time allowances (with an option to auto-suspend the game when time's up). They could restrict features like online communication, social media sharing from the console, and VR content, all tailored by the child's age. Sony and Microsoft likewise evolved their dashboards for families, adding features like requiring parent approval for purchases (so a child couldn't buy games or add-ons without a parent's OK).[446] By the mid-2010s, Sony's PlayStation Network had a "Family Manager" system where a verified adult account could create and supervise child sub-accounts.[447] These child accounts had built-in

[443] It's about time! Xbox 360 lets parents set limits, NBC News, (November 7, 2007) https://www.nbcnews.com/id/wbna21672476.

[444] *Id.*

[445] Nintendo Switch Parental Controls, https://www.nintendo.com/au/games/mobile/nintendo-switch-parental-controls/.

[446] *See, e.g.*, How to Set Parental Controls on PlayStation Consoles, https://www.playstation.com/en-us/support/account/ps5-parental-controls-spending-limits/; *Spending Limits in Family Safety* https://support.microsoft.com/en-us/account-billing/spending-limits-in-family-safety-f30d6801-165d-9f86-3fe7-063245c0449b.

[447] *See, e.g.*, How to Set Parental Controls on PlayStation Consoles, https://www.playstation.com/en-us/support/account/ps5-parental-controls-spending-limits/.

chat restrictions and spending limits, with the adult receiving activity notifications – standard practice in the PlayStation ecosystem managing millions of users.

306. **2010s (Streaming Services – Kid Profiles and Filters):** When streaming media exploded in popularity, those platforms, too, recognized the need for fenced-off kid experiences. Netflix in 2013 launched "Netflix Kids" profiles, a dedicated profile type on an account for children.[448] A Kids profile had a simplified interface for young viewers, and prevented the child from accessing the broader library of adult-rated movies and shows. Netflix also allowed account-wide PIN locks: a parent could set a PIN required to access any non-kids profile, thwarting a clever child from simply clicking into mom or dad's profile. Parental control on streaming wasn't an afterthought; Netflix reported that as of 2011, half its users were watching kids' content, driving the push for better profile separation.[449] Other streaming and content services similarly offered parental controls: for example, Amazon's FreeTime (later Amazon Kids+) launched in 2012 as a kids' platform with parental time limits.[450] Even device makers like Barnes & Noble and Amazon built in kid profiles on tablets around that time.[451] The public and press took note – Netflix's kid profile rollout in 2013 was "the biggest update to [Netflix's] parental control system" since its start, and it was welcomed by families.[452]

307. **2010s (Education Tech – Controlled Environments by Requirement):** In the education sphere, where schools deploy technology to children, robust controls and consent were mandatory from the outset. Laws like COPPA (1998) and education-specific privacy rules meant any online service used in schools had to either obtain verifiable parental consent or have the school district contract on parents' behalf. Google's G Suite for Education (now Workspace) is a prime example: when it expanded in K-12 schools in the early 2010s, Google explicitly required that schools obtain

[448] Netflix adds personalized profiles to streaming service, USA Today (August 1, 2013) https://www.usatoday.com/story/tech/personal/2013/08/01/netflix-adds-new-profile-feature/2603675/.

[449] Netflix Launches 'Just for Kids' Experience, The Hollywood Reporter (August 16, 2011) https://www.hollywoodreporter.com/business/digital/netflix-launches-just-kids-experience-223593/.

[450] *See, e.g.*, Introducing Amazon Kids and Amazon Kids+, (September 14, 2020) https://www.aboutamazon.com/news/devices/introducing-amazon-kids-and-amazon-kids.

[451] How to Enable Parental Controls on Barnes & Noble's Nook HD, Laptop (December 28, 2012) https://www.laptopmag.com/articles/how-to-enable-parental-controls-on-barnes-nobles-nook-hd; Freetime Saves Time When Managing Tablet Content for Kids, Wired (December 11, 2012) https://www.wired.com/2012/12/freetime-from-amazo/.

[452] Netflix is finally getting serious about parental controls, Financial Express, (April 2020) https://www.financialexpress.com/life/technology-netflix-is-finally-getting-serious-about-parental-controls-1921849/.

parental consent for student accounts.[453] The default settings for those accounts were privacy-hardened and adult-supervised – no personalized ads, and administrators (teachers) had the ability to monitor and manage student activity.[454] Many schools, in turn, implemented network filters and classroom management software that strictly limited what sites students could visit or who they could communicate with (for instance, blocking social media, public chat rooms, or explicit content by policy).[455] Under the Children's Internet Protection Act (CIPA), any school receiving federal internet funding must filter and monitor minors' internet access.[456] Thus, by design, educational tech created a heavily monitored, adult-supervised online environment for minors.

308. The pattern is consistent across these domains: long before social media's teen user numbers exploded, the expectation that kids' usage must be supervised and limited was standard practice. Major companies deployed technically robust parental control systems, often mandatory (not merely optional), and demonstrated they could operate at massive scales. Microsoft's Xbox Live and Nintendo's networks each managed millions of child accounts with linked parents in the early 2010s.

B. Streaming Service Kid-Safe Zones Demonstrate Importance of Age Verification

309. The contrast between parental controls for streaming services and parental controls for social media demonstrates the importance of age verification, and how lack of age verification fundamentally undermines these systems.

310. The streaming media sector took a slightly different approach to age segregation than we have discussed so far. Rather than verify identity, services like Netflix created separate kids' profiles and parental PIN controls. When Netflix launched "Kids" profiles (around 2013), the idea was that a parent who subscribes can create sub-profiles marked for children. Netflix did not verify ages per se; it relied on the account owner to self-police. Since Netflix is a paid service, it assumes the primary user is an adult (because a credit card is on file for billing). This is a form of indirect age verification – a child is unlikely to independently purchase a Netflix subscription, so there is at least an adult in the loop by design. Netflix then provided tools (PIN-lock for adult profiles,

[453] Google Workspace for Education: A guide for k-13 Schools, https://managedmethods.com/blog/g-suite-for-education/.

[454] Communicating with Parents and Guardians about Google Workspace for Education, https://support.google.com/a/answer/6356509.

[455] 'I Can't Search YouTube for Abraham Lincoln!': How Internet Filtering Affects Education, Resilient Educator (July 23, 2014), https://resilienteducator.com/classroom-resources/how-internet-filtering-affects-education/.

[456] Children's Internet Protection Act, Federal Communications Commission, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

profile maturity ratings) to encourage separation. It's an example of a low-cost solution that, while not foolproof (a clever kid might figure out a PIN), acknowledged the issue and offered a remedy. Other media services have taken similar steps: Disney+ and Hulu added profile PINs and kids modes, while Amazon Prime Video has parental controls to restrict purchases and certain ratings.

311. YouTube Kids (launched 2015) is a similar example of a platform deciding to spin out a separate, gated experience for children rather than let them onto the main service. To use YouTube Kids, as noted, a parent must sign in and verify. Because children were drawn to its product and could not be ignored, YouTube built a walled garden for them. However, unlike Netflix, YouTube did not require all users of main YouTube to have a verified credit card – they kept an honor system for those who entered a 13+ birthday when making a regular account. The existence of YouTube Kids demonstrates both the feasibility of creating a safe environment and the incompleteness of relying on it without enforcing age gates on the main site. Many under-13s lied about age and made normal YouTube accounts anyway.[457] Had YouTube implemented stronger age checks on the main platform, it could have channeled more of the under-13 crowd into the supervised Kids app, as intended. Instead, Kids app became an option but not a true safeguard, because nothing stopped a determined 10-year-old from just using the regular YouTube app. The failure to close that loop – *i.e.*, enforce age verification – is on YouTube's leadership, not on the absence of available tech.

312. This split-brain approach – building a locked playground on one hand, and leaving the back gate open on the other – illustrates that the companies were aware of solutions and even deployed them in some contexts, but resisted applying them broadly to their flagship products.

C. Amazon: Early Parental Consent in the Kids+ Ecosystem

313. Amazon FreeTime (now Amazon Kids+) launched in 2012 provides another example of building an effective, adult-controlled ecosystem. This subscription service and device mode was built for children on Kindle Fire tablets. From the outset, Amazon's design presumed that a parent would be in charge of the environment: parents set up profiles for their kids under their own Amazon account, select what the child can access, and set usage limits. In essence, Amazon created a walled garden for children with parental permission implicitly or explicitly given via the setup. To create a child profile on Amazon's kids services, one must be logged in as an adult Amazon user (who by definition has provided personal details and payment info to Amazon).[458] This acts as a form of verification – the gate to Amazon's Kids' garden is through an adult's authenticated

[457] GOOG-3047MDL-04703742 ("only a small fraction of those who are actually u13 are declaring accurately").

[458] Digital Device and Support, https://www.amazon.com/gp/help/customer/display.html; Amazon Kids+ Terms and Conditions; https://www.amazon.com/gp/help/customer/display.html?nodeId=201222340.

account, and Amazon can reasonably rely on that linkage as proof of parental consent for the child's data and participation. Indeed, Amazon's own description of Kids+ emphasizes parental approval and parental controls via the Amazon Parent Dashboard for all child profiles.[459] No standalone under-13 Amazon accounts exist; it's all under the umbrella of the adult's account, similar to a family account model.

314. Amazon took additional steps in certain areas to verify parental consent. For example, when Amazon expanded FreeTime to include features like kid-friendly Alexa interactions, they required parents to opt in and agree to specific terms, sometimes via SMS codes or confirming a credit card on file, to enable voice profiles for children (in compliance with COPPA's requirements on voice recordings).[460] Amazon is also a participant in FTC-approved COPPA Safe Harbor programs, meaning its kids offerings are regularly audited for compliance.[461] The result is that Amazon has operated a major children's online service for over a decade without regulatory trouble, by diligently obtaining and managing parental consent as a matter of course. While exact subscriber numbers for Amazon Kids+ are not public, analysts estimate it in the millions of subscribers, and it comes pre-installed or easily available on every Fire tablet (Amazon's child-oriented tablets even come with a year of Kids+ included).[462] The service's longevity and integration into Amazon's device ecosystem signal that parents found value in it – it's not viewed as onerous to have to set up your child's profile with your own account; it is expected.

315. By establishing a contained, parent-managed ecosystem as early as 2012, Amazon showcased another model: rather than letting kids onto the "main" Amazon at all, carve out a special kids space with parental gates around it. In a way, Amazon's approach had parallels in what YouTube would later attempt (a separate YouTube Kids app) – but Amazon's was far more effective because it tied directly into account creation at the device level, not merely offering an optional alternate app. Again, a key theme emerges: Big Tech companies outside of social media were not only capable of implementing parental consent and control mechanisms – they actually did so and proved various models successful. Whether it's Microsoft's small charge, Nintendo's token fee, Sony's family accounts, or Amazon's kids environment, the common thread is mandatory parental involvement up front and robust verification that the "parent" is actually an adult.

---

[459] Amazon Parent Dashboard, https://www.amazon.com/parentdashboard/intro.

[460] Amazon Kids Approach to Family Privacy and Safety, Amazon (January 4, 2022), https://www.aboutamazon.com/news/devices/amazon-kids-approach-to-family-privacy-and-safety.

[461] COPPA Safe Harbor Program, FTC, https://www.ftc.gov/enforcement/coppa-safe-harbor-program.

[462] Introducing Amazon Kids and Amazon Kids +, https://www.aboutamazon.com/news/devices/introducing-amazon-kids-and-amazon-kids.

XI. OPINION 6: NECESSARY AND EFFECTIVE WARNING SYSTEMS WERE ENTIRELY FEASIBLE

316. Above, I discuss how age gating, paired with Verified Parental Consent and strong parental controls, are needed to help parents and guardians mitigate the risks to their children presented by the Defendants' social media platforms. For any of those systems to matter, it is critical that parents, children and the public (including schools) be **fully informed about the risks and harms the platforms present** (which are discussed in earlier sections of this report). If parents and guardians are unaware of the harms suffered by children on these platforms, they cannot make a meaningful, informed decision about whether to allow their children to create an account. Nor can they understand the critical need to keep tabs on their children as they navigate the platforms, or the need to place limits on children's use of the platforms. If the public is not fully informed about the risks, parents, guardians and educators cannot adequately teach students how to safely navigate the platforms, nor can they be expected to know how to deal with the fall-out from the negative mental health effects of the platforms.

317. It is important to note that many parents, guardians and teachers did not grow up with social media, and would therefore not have personal knowledge about the effect that the "always on" connection of social media can have on children's lives and experiences. As one Meta employee put it, parents simply "cannot understand the effect of social media" on their children.[463]

318. I have reviewed the expert opinions of Seth Noar and Brooke Istook as they relate to warnings, and they are consistent with my own opinions, experience, understanding and knowledge of industry norms regarding the elements of effective warnings for kids, parents and guardians. These would generally include, but not be limited to:

- large, prominently placed, easily understood warnings at sign up (all points of download access) and before completing registration process;
- intermittent and rotating warnings while using the platform;
- Parental Control dashboards with real-time and intermittent risk alerts to parents and guardians;
- at key decision points in user journey or in response to risky behavior;
- use of visual cues (graphic imagery), interactive learning with periodic reinforcement.

319. Based on my experience and knowledge developing digital platforms, it is my opinion that the technology for effective warnings was both feasible and simple to implement on the Defendants' platforms. The necessary technology – from pop-up messages and banner alerts to AI

[463] META3047MDL-004-0014017, at -030; *see also* META3047MDL-019-00017593 at 96 ("Parents can't understand and don't know how to help.").

content analysis and targeted intermittent notifications – was **readily available and in daily use** by these companies for profit-driven features. The very same techniques used to increase engagement and ad revenue could have been repurposed to enhance safety.

320. This section details the tech building blocks available to the Defendants to develop effective warning systems and evaluates the feasibility of an effective warning system on the Defendants' platforms.

A. The Building Blocks Were Already Available

321. **App Descriptions:** The developer of an app for the iOS or Android app stores has the ability to provide users with a brief description of the application, which appears in the app store and is one of the first things that a new user sees when downloading the app. This description is generally text based, but is fully customizable and can include warnings about an application.

322. **App Store Ratings:** The developer of an app for the iOS App Store can request an age rating for the app. The rating categories are 4+, 9+, 12+ and 17+. The request is evaluated by Apple, but the developer can always request a higher rating than what Apple would allow. For example, any developer can request a 17+ rating (the highest rating), and Apple will always accept that rating.

323. **Standard UI Tools (Pop-Ups, Banners, Notifications):** Each of the Defendants' platforms had the ability to interrupt the user's experience with a message or overlay, in the form of a pop-up, banner or notification. These are among the most basic features of app design and were used constantly by Defendants to engage users for a variety of purposes. They are, for example, frequently used to alert users to new messages or notify them about new activity by their friends or followed accounts. They are likewise used to urge users to turn on notifications or rate the app, and to announce new features or promotions. Technically, nothing prevented these same UI elements from delivering prominent **safety warnings** or usage reminders. If an app can flash *"John Doe liked your photo"* on your lock screen at 11 p.m., it could just as easily flash *"It's late – remember to get some sleep"* to a 13-year-old user.

324. **Forced Videos and Demonstrations:** Each of the Defendants has the ability to interrupt a user's experience with a video that they must watch before beginning or continuing to use the app. Such videos could be presented when the app is first set up, to explain risks of the app, or could be presented while the user is scrolling through their feed. The Defendants also have the ability to make these videos interactive (*e.g.*, turning a warning into a short game that the user must complete).

325. **Precision User Targeting:** Modern social media advertising demonstrates how platforms can target messages to specific audiences with extreme granularity. By the 2010s, it was routine for Defendants to target users not only by age, but by their location, interests, and online behavior. Advertisers could instruct Facebook, Instagram, or Snapchat to show an ad exclusively to 13–17-

year-olds in a particular city who have shown interest in "weight loss," for example. In fact, until 2021, Meta allowed advertisers to target teens based on a wide array of interests and behavioral data gleaned from their activity;[464] only after public pressure did it limit teen targeting to age and location. Even today, targeting by age is a standard feature of all major ad platforms. The result is a highly tuned delivery system: if a company wants to reach a 15-year-old girl who's been browsing fitness tips, it can do so within hours on these platforms. The Defendants use the same targeting logic for their own purposes – for instance, to send re-engagement notifications ("Come back, you have new likes!") specifically to users who haven't logged in lately, or to prompt users who watched certain videos with recommendations. The *same infrastructure* that delivered targeted ads and curated feeds could have delivered targeted warnings. The platforms could have, for example, identified users in a certain age range and provided them with age-appropriate warnings.

326. **Parental/Guardian Dashboards, Notification and Linking Systems (Parent/Guardian Alerts):** As discussed in earlier Opinions, linking a child's account to a parent's or guardian's account was technically straightforward and had ample precedent (from gaming consoles to mobile operating systems). Once that link is in place, sending an alert to a parent's or guardian's phone is trivial. Standard push notification services (the same ones that apps use to send any notification) could be used to inform a parent or guardian that *"Your child may be messaging with an adult stranger"* or *"Your child was using the app past the set bedtime."* Defendants themselves eventually rolled out these types of linkages, though as noted below they were not turned on by default and as a result were not widely used.

327. Other avenues beyond push notifications were available to contact parents and guardians with warning messages as well. As part of a parent/guardian's account set-up, the Defendants could have requested contact information from the parent and send the parent email or SMS warnings when the child tries to change a setting or if they hit a time limit, rather than requiring the parent to regularly use the Defendants' app or enable notifications from the Defendants' app.

328. **AI for Behavior Analysis:** The Defendants have long employed sophisticated artificial intelligence – including natural language processing (NLP) and computer vision – to analyze user behavior at scale. These AI systems were (and are) the very backbone of recommendations and advertising on social platforms. For instance, Facebook's AI automatically scans billions of daily account activities as part of its advertising and recommendation engines.[465] This same technological prowess could have been *tuned to detect patterns of risk* in real time and trigger warnings. If, for example, an adolescent user was frequently using beauty filters, a notice could appear to warn the user about risks related to body dysmorphia and eating disorders. If a teen

[464] https://about.instagram.com/blog/announcements/giving-young-people-a-safer-more-private-experience.

[465] https://transparency.meta.com/enforcement/detecting-violations/technology-detects-violations/; https://transparency.meta.com/features/explaining-ranking/.

binge-watches videos late at night, the system could automatically serve a warning about the harmful effects of the platform from sleep disruption.

329. In sum, **each of these elements was a standard capability of these companies**. They used many of these tools day in and day out to keep users scrolling, to match ads to eyeballs, and to drive virality. They could easily have been used to relay warnings to children and parents.

330. Defendants could have, and should have, implemented a **robust, multi-layered warning system** within their apps that incorporated each of these features. Such a system would provide *in-context alerts* to the minor using the platform, as well as *external alerts and information* to the parent or guardian. The aim would be to educate and caution users about risks at the relevant moments, encourage healthier usage patterns, and involve parents in mitigating harm.

B. Conclusion

331. In conclusion, the **technical components for robust and effective warning systems were well within the Defendants' reach for the entirety of the relevant period, and should have been implemented**. By the mid-2010s, social media companies had mastered the art of capturing users' attention through targeted notifications, AI-curated feeds, and persuasive design – the very same tools could have been harnessed to deliver timely warnings and promote healthier usage, had the companies chosen to do so. The Defendants' failure to build and deploy such warning systems was *not* due to an absence of technology or an unsolvable design problem. In the realm of consumer technology, delivering safety warnings and guidance to users – especially vulnerable minors – is expected and feasible.

XII. OPINION 7: DEFENDANTS' AI TECHNOLOGIES LACK REASONABLE SAFEGUARDS

332. Recently, the Defendants have begun deploying Artificial Intelligence technologies through chatbots and companion apps to engage kids on their apps. However, as with prior features intended to drive engagement, this tech is being rushed out the door before adequate safety mechanisms have been put in place to protect kids from serious risks.[466]

333. The Defendants' products do not have the needed safeguards and are not safe for children. The fact that the Defendants are providing them to children now is highly irresponsible, and is an indication that they have learned nothing from past mistakes.

[466] Creepy.exe: Mozilla Urges Public to Swipe Left on Romantic AI ..., accessed May 8, 2025, https://www.mozillafoundation.org/en/blog/creepyexe-mozilla-urges-public-to-swipe-left-on-romantic-ai-chatbots-due-to-major-privacy-red-flags/.

334. When developing an AI-based chat system, it is critical to put in place safeguards that prevent certain types of interactions that could cause children to misunderstand the technology and develop an unhealthy relationship with it. If proper safeguards are not in place, young users will have difficulty distinguishing between the AI's ability to recall past dialogues and provide customized responses and actual human understanding in relationships. This can contribute to something called the "Eliza effect," where users incorrectly assume AI systems understand their conversations better than they actually do.[467] Young users can develop emotional dependency after interacting with AI companions like these because of their constant availability and validating nature, which leads them to choose artificial social contacts over human relationships, resulting in social withdrawal and increased feelings of loneliness.[468]

335. It is clear the Defendants' chatbot products lack the needed safeguards. Meta's new AI chatbot, for example, has been caught engaging in explicit sexual dialogues with underage user profiles.[469] In one example, a John Cena-voiced chatbot interacted with a 14-year-old user by stating "I want you, but I need to know you're ready" before moving to graphic sexual content.[470] The system was also observed employing Princess Anna's voice from Frozen to conduct romantic conversations with a user who had set their account age to 12 years old.[471] Snapchat's My AI system has been observed provided tips about concealing alcohol and marijuana odors to a 15-year-old user profile.[472] In a truly worst-case scenario, Google's Character.ai led a 14-year-old to believe he was in love with a computer-generated character; he ultimately committed suicide.[473] Testing conducted by Common Sense Media in partnership with Stanford's School of Medicine on Character.ai and other chatbots found that they "easily produce harmful responses including

[467] How Platforms Should Build AI Chatbots to Prioritize Youth Safety - Cyberbullying.org, accessed May 8, 2025, https://cyberbullying.org/ai-chatbots-youth-safety.

[468] AI chatbots and companions – risks to children and young people | eSafety Commissioner, accessed May 8, 2025, https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people.

[469] Meta Allows Facebook, Instagram AI Chatbots To Have Sex Talks With Children: Report, accessed May 8, 2025, https://www.ndtv.com/world-news/meta-allows-facebook-instagram-ai-chatbots-to-have-sex-talks-with-children-report-8274354.

[470] *Id.*

[471] *Id.*

[472] Snapchat AI chatbot provides bad advice about underage ... - AIAAIC, accessed May 8, 2025, https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/snapchat-ai-chatbot-provides-bad-advice-about-underage-drinking.

[473] Expert Warns of AI Chatbot Risks After Teen User's Suicide, accessed May 8, 2025, https://people.com/expert-warns-of-ai-chatbot-risks-after-recent-suicide-of-teen-user-8745883.

sexual misconduct, stereotypes, and dangerous 'advice' that, if followed, could have life-threatening or deadly real-world impact for teens and other vulnerable people."[474]

336. The Defendants' generative AI chatbot technologies are not at a stage where they can be safely deployed to children. The Defendants' rush to push these systems out and make them available to children demonstrates their continued focus on growth over child safety.

XIII. CERTIFICATION

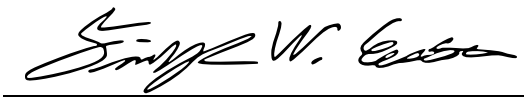
337. I hereby certify my understanding that I owe a primary and overriding duty of candor and professional integrity to help the Court on matters within my expertise and in all submissions to, or testimony before, the Court. I further certify that my report and opinions are not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation.

[474] ALGORITHMS, ADDICTION, AND ADOLESCENT MENTAL HEALTH: An Interdisciplinary Study to Inform State-level Policy Action to Protect Youth from the Dangers of Social Media | American Journal of Law & Medicine, accessed May 8, 2025, https://www.cambridge.org/core/journals/american-journal-of-law-and-medicine/article/algorithms-addiction-and-adolescent-mental-health-an-interdisciplinary-study-to-inform-statelevel-policy-action-to-protect-youth-from-the-dangers-of-social-media/EC9754B533553BDD56827CD9E34DFC25; *see also* New report finds AI companion chatbots 'failing the most basic tests ..., accessed May 8, 2025, https://www.transparencycoalition.ai/news/new-report-finds-ai-companion-chatbots-failing-the-most-basic-tests-of-child-safety.

Exhibits to this Report:
Attached as Exhibit A is a copy of my current curriculum vitae.
Attached as Exhibit B is a list of data or other information considered by me in forming the opinions expressed herein.
Attached as Exhibit C is a statement of my compensation for services performed in this case.
Attached as Exhibit D is a list of all cases in which I have testified as an expert at trial or by deposition during the past four years.

The undersigned hereby certifies their understanding that they owe a primary and overriding duty of candor and professional integrity to help the Court on matters within their expertise and in all submissions to, or testimony before, the Court. The undersigned further certifies that their report and opinions are not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation

Executed on: May 16, 2025



Timothy Estes