Exhibit B

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

IN RE: SOCIAL MEDIA ADOLESCENT ADDICTION/PERSONAL INJURY PRODUCTS LIABILITY LITIGATION THIS DOCUMENT RELATES TO: *People of the State of California, et al. v. Meta Platforms, Inc., et al.*	MDL No. 3047 Case Nos. 4:22-md-03047-YGR-PHK 4:23-cv-05448-YGR Judge Yvonne Gonzalez Rogers

EXPERT REBUTTAL REPORT OF MARY CATHERINE WIRTH

January 9, 2026

TABLE OF CONTENTS

I. SUMMARY OF EXPERT OPINION

1. I have been retained by counsel for Meta Platforms Inc. ("Meta") to review and respond to the expert reports[1] of Dr. Patrick McDaniel -- specifically, his opinion that Meta's age assurance practices fail to meet applicable standards. My opinions are summarized below.

A. Opinion 1: U.S. Internet Companies Look To Privacy and Trust & Safety Professionals For Age-Gating Expertise

2. In my experience, U.S.-based internet and social media companies rely on privacy program managers or trust and safety professionals for guidance when designing their age-gating workflows. At large technology or social media companies, age-gating development and operation is principally considered a privacy compliance and/or Trust & Safety program management issue, not an engineering one.

3. When designing age-gating mechanisms, U.S. companies typically rely on an in-house Chief Privacy Officer (CPO), Certified Information Privacy Professionals (CIPPs) and/or their in-house privacy program manager for advice on how to develop and operationalize an age gate that is both compliant and consistent with industry best practice.

4. Similarly, developing a program for enforcing a company's Terms of Service (including terms forbidding platform use by those under the age of 13) is the purview of Trust & Safety professionals and the various in-house and outsourced moderation and enforcement staff that they train and oversee.

B. Opinion 2: U.S. Companies Design Their Age-Gating Programs In Accordance With Long-Standing FTC Staff Guidance and Voluntary Industry Best Practices

5. In the U.S., age-gating practices across large social media and Internet platforms are highly uniform for two very practical reasons:

- First, Federal Trade Commission (FTC) staff has, for many years, published fundamental age-gating guidance for U.S. businesses online in plain language written for non-lawyers.

[1] This report responds both to Dr. McDaniel's November 21, 2025 Trial Report and his December 15, 2025 Corrected Trial Report.

That guidance has remained substantively stable for decades. As a result, certain age gating "fundamentals" have become commonly understood, industry-wide operational reference points for the privacy program managers and Trust & Safety professionals who are responsible for designing and overseeing age-assurance workflows and moderation programs at U.S. technology companies.

- Second, in recent years, collaboration among larger platforms has led to a set of voluntary industry age assurance "best practices" that mature programs typically layer on top of these stable and long-accepted age-gating "fundamentals."

6. Because published FTC staff guidance on age gating has been so stable and long-accepted in the industry, and because most large U.S. platforms have collaborated closely on best practice development, there is a uniquely high degree of industry conformity around U.S. age-gating operations. In my experience, age gates at every major U.S. platform – from Facebook to Instagram to Google to Microsoft to Snap to TikTok – are virtually identical to one another in functionality.

7. Dr. McDaniel does not acknowledge this reality. His report never once mentions the FTC staff's plain-language guidance that has shaped age gating practices at U.S. companies for decades. And despite offering an opinion that Meta's age gating practices are insufficient, Dr. McDaniel does not, at any point, examine or compare age gating practices among other major U.S. social media platforms.

C. <u>Opinion 3</u>: NIST and IEEE Engineering Standards Are Neither Relevant To, Nor An Accepted Measure of, U.S. Age Gating Best Practices

8. Rather, over the course of his 100+ page report, Dr. McDaniel examines and applies various National Institute of Standards and Technology ("NIST") and Institute of Electrical and Electronics Engineers ("IEEE") engineering standards. He then explains the various ways he believes Meta fails to meet those engineering standards.

9. Yet neither standard applies to Meta's age gating practices (or to the practices of any other U.S. based social media or internet company offering services to the general public). This is because:

- NIST standards are binding only on federal government agencies. They do not apply to commercial general-audience online websites or internet services offered to the public at large. Indeed, the FTC expressly rejected a request that it adopt the NIST Privacy Standard as its definition of "reasonable" operator behavior under COPPA earlier this year – preferring, instead, to leave that definition more "flexible."[2]

- IEEE voluntary age verification standards were developed to guide engineering best practices in nations *outside* of the U.S. (*i.e.,* the U.K., Australia and Indonesia) where age verification is now mandated by law. They do not apply to U.S-based companies doing business in the U.S., where age verification is not yet mandated by law.[3]

10. Dr. McDaniel never provides a single example of any U.S.-based social media or internet company that complies with the NIST and IEEE standards he describes at such length. The reason for this is straightforward: ***he doesn't because there is no such example.*** To my knowledge, not one U.S.-based social media or internet company that provides services to the general public looks to the NIST or IEEE standards Dr. McDaniel cites as the source (or even "a" source) of its U.S. age-gating obligations.

D. Opinion 4: Meta's Age Gating Programs Meet (and Often Exceed) Industry Accepted Standards & Best Practices

11. Based on my review of Meta's public-facing documentation and discovery materials in this case, it is my professional opinion that Meta's age assurance practices for Facebook and Instagram meet (or exceed) applicable U.S. industry standards and best practices. Meta follows long-accepted FTC staff guidance to businesses regarding using a neutral age gate at account signup. It also has well-defined processes for identifying and removing users once it has actual knowledge that they are under the age of 13.

---

[2] Children's Online Privacy Protection Rule, 90 Fed. Reg. 16961 (Apr. 22, 2025).

[3] *See, e.g.,* Alex LaCasse, *Are new global age verification requirements creating a children's online safety legal patchwork?*, Int'l Ass'n Priv. Pros. ("IAPP") (August 14, 2025) (describing the age-verification requirements for the European Union, Australia, and the United Kingdom, and noting European Union and the fact that U.S. law still does not mandate similar efforts), https://iapp.org/news/a/are-new-global-age-verification-requirements-creating-a-children-s-online-safety-legal-patchwork-.

12. Meta also takes the "layered" industry best practice approach to age-related enforcement. For example, it (a) uses technical measures to prevent users who have failed an age assurance test from circumventing the controls, (b) uses machine-learning classifiers trained on reliable signals to flag underage accounts, (c) accounts flagged as potentially underaged are either immediately actioned (where there is a high degree of confidence in accuracy) or "checkpointed" and escalated to highly trained human moderators for review (where there is lower confidence), (d) "checkpointed" accounts are no longer accessible to the user or visible to other users during the evaluation process, (e) accounts that fail the age checkpoint are closed and their data is deleted once the appeal period has expired, (f) accounts linked to the failed account (for example, a Facebook account linked to an Instagram account) are also closed and deleted, (g) a user changing their self-declared age from under 18 to over 18 triggers a more robust age verification check by a third party account verification vendor, (h) accounts also are automatically checkpointed if a user changes their self-declared from over 13 to under 13, (i) users and the general public can report directly to Meta that a particular user is under the age of 13, and (j) the company has implemented "Teen Accounts" on both Instagram and Facebook, which default to protective settings and offer parents suitable account controls.

To the extent that Dr. McDaniel comes to a different conclusion, it is because he fails to measure Meta's practices against accepted, published industry best practices. Rather, he calls Meta's efforts "inadequate" because they do not reflect the outer limits of what is "technically feasible." But – as with NIST and IEEE engineering standards – "technical feasibility" is not an accepted benchmark or standard for evaluating the adequacy of an age assurance (or any other) Trust & Safety program.

II. BACKGROUND AND QUALIFICATIONS

13. I have been advising large internet and technology companies on children's privacy and Trust & Safety matters for more than two decades, including overseeing the development, implementation and day-to-day operation of compliant age-gating mechanisms and the removal of underage accounts when a site obtains actual knowledge that a specific user is under the age of 13.

14. In this matter, I was asked by Meta to review and respond to the expert reports of Dr. McDaniel. Specifically, I was asked to (a) review and, where necessary, rebut Dr. McDaniel's opinion regarding Meta's age assurance practices; (b) offer my expert opinion regarding industry age-gating best practices and standards; and (c) evaluate Meta's practices against those best practices and standards.

A. Education

15. I graduated with a B.A. in History from the University of California, Davis in 1989 and a Juris Doctor degree from University of California, Hastings College of the Law in 1992. In 2013, I passed the International Association of Privacy Professional's Certified Information Privacy Professional/United States (CIPP/US) exam and became a certified privacy professional.[4]

B. Work Background

16. After law school graduation, I focused on Media and First Amendment law, first as a litigation associate at O'Melveny & Myers and later in-house for News Corporation (1992-1997). From 1997-2000, I was a trial lawyer in the litigation department of the law firm of McCutchen, Doyle, Brown & Enersen. In August 2000, I left McCutchen to take an in-house role overseeing all of Yahoo! Inc.'s international litigation, law enforcement response, compliance and content policy work. As part of my responsibilities at Yahoo!, I advised the company on international privacy requirements and supervised our international websites' operationalization of those requirements. I also coordinated with our domestic compliance team and Chief Privacy Officer to ensure our international and U.S. obligations were harmonized wherever possible.

17. In mid-2006 I became a mom and left Yahoo! From 2006 – 2008, I stayed home to focus on parenting. I continued teaching an international cyberlaw seminar at U.C. Hastings College of the Law during this time. I also served as an informal legal advisor and mentor to YouTube's first General Counsel as she began navigating the same type of complex content moderation and compliance issues we navigated at Yahoo!

[4] *See CIPP/US: Certified Information Privacy Professional/United States*, IAPP, https://iapp.org/certify/cippus/

18. In the spring of 2008, I received a call from a lawyer who had been the head of Yahoo!'s European legal team, who now was heading up the European legal team for software maker Adobe. He told me that Adobe was at the very beginning of planning a business model transformation: from traditional software provider to cloud-based "Software as a Service" ("SaaS") delivery and storage. At the time, the company's legal department was relatively small and was made up primarily of traditional software licensing lawyers. The company needed to bring in someone with substantial experience overseeing a global internet / user-generated content-based compliance program to advise their General Counsel and executive team. After meeting with the General Counsel, I was hired initially as a consultant and then, later, full-time as the company's first Head of Trust & Safety.

19. My initial role at Adobe was to guide the company's general counsel and executive team through the "hosted services" aspect of this business transformation, as well as the development of the various new policies, compliance programs and technology integrations that the company would need to build from scratch as it began transitioning to this new business model. I also oversaw the development and launch of what eventually became the Adobe Trust & Safety program – leading a blended team of lawyers, program managers, internal and outsourced moderation staff and, eventually, a dedicated Trust & Safety engineering team.

20. For most of my time at Adobe, I reported to the company's Chief Privacy Officer, and our combined team was called "Privacy Trust & Safety." Ultimately, the company launched the Adobe "Creative Cloud" in June 2013 and a variety of other hosted services thereafter.[5]

21. During my 11 years at Adobe, I was the executive primarily responsible for all children's privacy and safety initiatives globally, including compliance with the COPPA Rule and industry best practices, guiding the company's Identity & Authentication team through development of our registration and age-gating workflows, as well as modifying those workflows as appropriate for Create Cloud sold to government and private K-12 education. To be effective in my role, I needed deep expertise regarding the rules and standards that applied to the company in its

[5] Adobe's successful pivot from traditional software provider to a thriving, cloud-based subscription-based business is widely lauded as "one of the most ambitious and successful business model transformations in modern corporate history" – taking it from a market capitalization of $16 billion pre-transition to well over $200 billion afterwards. Robbie Baxter, *A Behind-The-Scenes Look at Adobe's Journey to Subscriptions*, Medium (2025) https://medium.datadriveninvestor.com/a-behind-the-scenes-look-at-adobes-journey-to-subscriptions-c720acac814e.

position as a general audience website that excluded users under the age of 13 from registration (*i.e.,* subscription services made available to the general public via the company's website). And I needed equally deep expertise about additional rules and standards that came into play when we provided hosted services to enterprises, to federal and state governments, and to public schools.

22. As the company's Head of Trust & Safety, I also worked with our engineering teams to develop classifiers and trust algorithms to help us better detect users who were likely to engage in a variety of different terms of service violations, including attempts to evade our age gating mechanisms. And I developed training for our moderation staff regarding how to manage situations where we obtained actual knowledge that a specific user was under the age of 13.

23. While at Adobe, I studied for and passed the IAPP's Certified Information Privacy Professional (US) exam, thereby obtaining my CIPP/US professional designation. While at Adobe, I also routinely kept up with industry privacy best practices by attending IAPP conferences and seminars and by networking with other in-house privacy professionals.

24. I left Adobe in 2019 to, once again, prioritize parenting. However, without any particular intention of doing so, I ended up in a consultancy role. I don't advertise or actively seek work. I don't have a website. I don't write articles. I only occasionally agree to speak publicly on child safety topics.[6] But, because I have been doing internet Trust & Safety and compliance work for so long,[7] and have mentored so many others at tech companies over the years, work just finds me – usually via an executive I have advised, a former work colleague who has moved to a new company or a peer at another tech company who I know through various industry associations like the Technology Coalition or the IAPP. My consultations most frequently are with companies who have either discovered they have a problem with child sexual abuse material (CSAM) on their platform or are contemplating the introduction of a new feature or business

[6] For example, I recently spoke on Teen Online Safety and AI at Stanford Law School's 22nd Annual "Digital Best Practices Conference. See *Mary Catherine Wirth Biography*, Stanford Law School, https://conferences.law.stanford.edu/bestpractices2025/speakers/mary-wirth/ ("Teens, AI Games & Social Media).

[7] Deirdre Mulligan, the long-time Director of the UC Berkeley Center for Law & Technology and the U.S. Principal Deputy Chief Technology Officer during the Biden administration, once spontaneously tweeted that I was one of three people who have been doing Trust & Safety work longer than anyone else in tech. *See, e.g., Professor Deirdre Mulligan Returns From White House To Teach Next Generation of Public Interest Technologists*, UC Berkeley School of Information, https://www.ischool.berkeley.edu/news/2024/professor-deirdre-mulligan-returns-white-house-teach-next-generation-public-interest; Deirdre K. Mulligan (@DMulliganUCB), X (Apr. 28, 2022 at 1:43 PM ET) https://x.com/DMulliganUCB/status/1519734028378656768.

model that has the potential to introduce one. However, I have also continued to advise companies on children's privacy, data security and safety matters, including overseeing recently settled multi-state AG and FTC litigation for a K-12 education technology company that suffered a major data breach.[8]

25. In consideration for my work in this case, I am being compensated in the amount of $1,000 per hour. My compensation does not depend on my opinions or the outcome of this litigation.

26. I am concurrently engaged as an expert witness for Meta in another pending litigation in New Mexico on the topic of both anti-CSAM program operation and U.S. age-gating best practices.[9] That is my only other expert engagement within the last four years.

III. OVERVIEW OF LONG-ESTABLISHED U.S. AGE GATING FUNDAMENTALS AND MORE RECENT INDUSTRY BEST PRACTICES

27. The opinions offered in this report are rooted in my own first-hand, practical experience as a CIPP, Trust & Safety executive and practitioner who has overseen the design of age gating programs, managed the staff overseeing their day-to-day operation, benchmarked best practices with privacy and Trust & Safety professionals at peer companies, worked with moderation teams to develop workflows and training materials to support program enforcement activities and advised in-house product and engineering teams on how to implement best practices in a variety of real-world industry settings, including (1) general audience websites and hosted services that preclude under 13 registration via neutral age collection mechanisms; (2) enterprise services sold to businesses or to the federal government and (3) in public and private K-12 school settings where users under the age of 13 are an intended part of the user base.

[8] *See* National Law Review, *"Connecticut, California and New York Reach Landmark Settlement for Student Data Breach"* (Dec. 2, 2025) https://natlawreview.com/article/connecticut-california-and-new-york-reach-landmark-settlement-student-data-breach; and Education Week Market Brief, *"FTC Takes Action Against Ed-Tech Company for Failure to Deliver on Security Promises"* (Dec. 4, 2025). https://marketbrief.edweek.org/regulation-policy/ftc-takes-action-against-ed-tech-company-for-failure-to-deliver-on-security-promises/2025/12.

[9] *State of New Mexico v. Meta Platforms, Inc.*, State of New Mexico, First Judicial District Court, Santa Fe County, No. D-101-CV-2023-02838.

A. Age Gating Mechanisms Across U.S. Platforms Are Highly Uniform Because FTC Staff Guidance To Businesses Is Very Detailed, Plain Language And Has Remained Unchanged For Decades

28. The design and baseline functionality of any U.S. platform's age assurance program is dictated primarily by long-standing FTC staff guidance on the COPPA Rule, as set forth in its plain language FAQs for businesses.[10]

29. Because FTC staff guidance for businesses is highly detailed, made available online in plain language for non-lawyers, and has remained virtually unchanged for decades, U.S.-based privacy program managers and Trust & Safety professionals who oversee age assurance program development and operations uniformly are familiar with its core age-gating fundamentals:

- **Platforms Must Collect Age Neutrally:** Platforms may ask users to self-declare their date of birth at registration or screen out any user who declares an age under 13, but the mechanism for doing so must be "neutral" — that is, it cannot encourage users to misrepresent their age. [11]

- **Platforms May Rely on Self-Declared Age:** Where age is collected neutrally, platforms may rely on self-declared age – even where the age declared by the user is false.[12]

---

[10] *See Complying With COPPA: Frequently Asked Questions ("COPPA FAQ")* https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (although the COPPA FAQ "represents the views of FTC staff and is not binding on the Commission," companies and practitioners have relied on its straightforward, plain-language guidance for decades).

[11] *Id.* at D.7 ("In designing your age screen, you should ask age information in a neutral manner, making sure the data entry point allows users to enter their age accurately and does not default to an age 13 or over. An example of a neutral age screen would be a system that allows a user freely to enter the month and year of birth. Avoid encouraging children to falsify age information by, for example, stating that certain features will not be available to users under age 13. In addition, consistent with long standing Commission advice, FTC staff recommends using technical means, such as a cookie, to prevent children from back-buttoning to enter a different age.")

[12] *Id.* at A.12. ("Will the COPPA Rule prevent children from lying about their age to register for general audience sites or online services whose terms of service prohibit their participation? No. COPPA covers operators of general audience websites or online services only where such operators have actual knowledge that a child under age 13 is the person providing personal information. The Rule does not require operators to ask the age of visitors. However, an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate. In some circumstances, this may mean that children are able to register on a site or service in violation of the operator's Terms of Service. If, however, the operator later determines that a particular user is a child under age 13, COPPA's notice and parental consent requirements will be triggered.")

- **Platforms Have No Obligation To Investigate or Verify Age Absent Actual Knowledge That A Specific User Is Under 13:** Platforms may be generally aware that they have underage users who gained access by declaring a false age at registration. However, a platform has no affirmative obligation to proactively investigate or verify an account holder's age unless or until they obtain actual knowledge that a *specific* account belongs to a child under 13.[13]

Although the FAQs may have their origins in law (*i.e.,* COPPA), they were developed by FTC staff for practical business operational use – *i.e.,* for use by small business owners, app developers, user experience designers, privacy program managers and moderation staff.[14] For this reason, understanding and applying them does not require any particular legal expertise.[15] Because these principles are, in my experience, universally accepted in the U.S. Privacy and Trust & Safety professional communities and have informed operational practices for decades, that is how they are incorporated into my opinion (*i.e.,* as long-standing accepted principles of U.S. age-gating program development and operation, not as any particular interpretation of the underlying law on which they are based).[16]

30. Because FTC staff guidance has always been so clear, plain language and stable, it is no surprise that that registration age-gating practices across large US-based internet platforms are highly uniform. Register for an account on Facebook, Instagram, Google, X, or TikTok and you will find highly similar neutral age "self-declaration" screens on each:

---

[13] *Id.* at H.6. ("The COPPA Rule applies to an operator of a general audience website if it has actual knowledge that a particular visitor is a child. If a child posts personal information on a general audience site or service but does not reveal her age, and if the operator has no other information that would lead it to know that the visitor is a child (such as the child posting that she attends an elementary school), then the operator would not be deemed to have acquired "actual knowledge" under the Rule and would not be subject to the Rule's requirements. Even where the child does reveal age-identifying information, if no one in an operator's organization is aware of the post, then the operator does not have the requisite actual knowledge under the Rule. However, you may be considered to have actual knowledge where a child announces her age under certain circumstances, for example, if you monitor user posts, if a responsible member of your organization sees the post, or if someone alerts you to the post (e.g., a concerned parent who learns that his child is participating on your site). Where an operator knows that a particular visitor is a child, the operator must either meet COPPA's notice and parental consent requirements or delete the child's information.")

[14] The FTC repeatedly emphasizes that the goal of its Business Center, where the COPPA FAQs reside, is to provide plain-language guidance to "help businesses understand their responsibilities." *FTC Business Guidance* https://www.ftc.gov/business-guidance.

[15] Indeed, most Trust & Safety professionals (and many CIPPs and CPOs) are not lawyers.

[16] This is why I have limited my recitation of these principles to direct quotes from the FTC's Business Guidance center, without citation to the underlying statute or case law interpreting it.

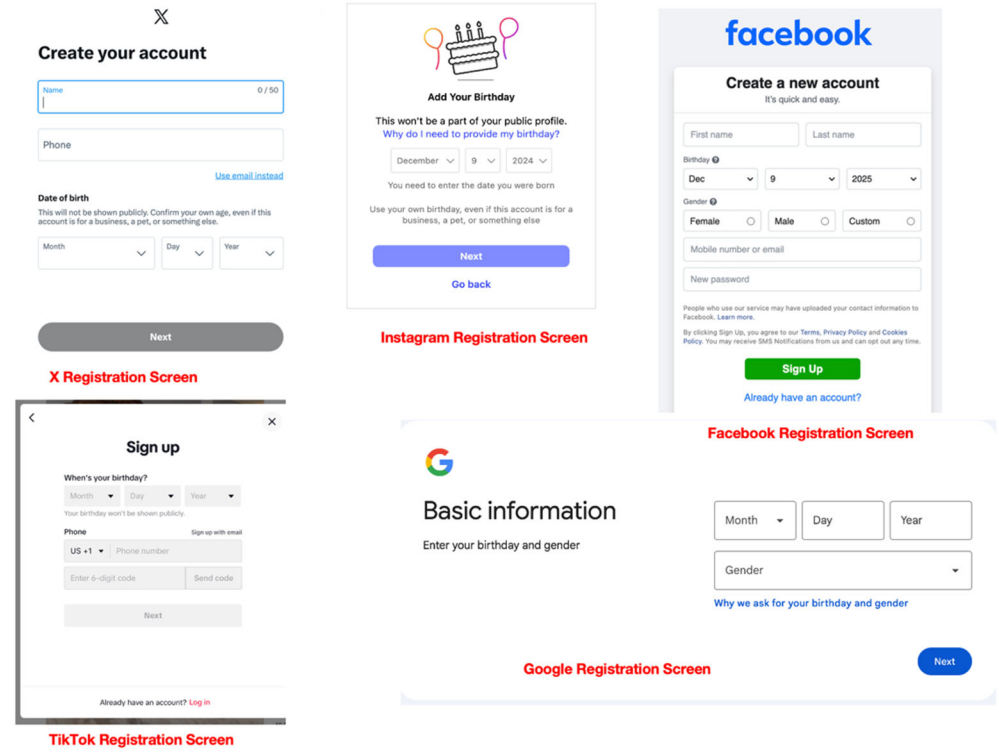


Figure 1-- Neutral Registration Age Gates On X, TikTok, Facebook, Instagram and Google. (Screenshots taken on Dec. 9, 2025).

To my knowledge, all large U.S.-based platforms that provide services to the general public allow neutral self-declaration of age and then rely on the age declared at registration. **Not one requires any form of more robust age verification at registration.**[17]

B. Larger U.S. Based Platforms (Like Meta) Voluntarily Do Far More Than FTC Guidance Requires

31. Although U.S. platforms are entitled to rely on self-declared age and have no proactive obligation to further investigate age absent actual knowledge that a specific account owner is under 13, many larger platforms – like Meta – voluntarily do much more.

[17] The only exception I know to this rule is for pornography-focused websites, which conduct more robust age verification at registration either voluntarily (for example, Only Fans – which does so at the behest of its voluntary compliance monitor) or to comply with recently enacted state laws like Texas H.B. 1181 (2023), which mandates more robust age verification at registration for websites where 33% or more of a platform's content is pornographic / harmful to minors. Texas H.B. 1181 was upheld as constitutional by the U.S. Supreme Court last summer in *Free Speech Coalition, Inc. v. Paxton*, No. 23-1122, 606 U.S. ___ (2025).

32. Until fairly recently, that voluntary "more" traditionally was developed by each platform independently and in isolation. This was a result of a long-standing challenge in the Trust & Safety field -- *i.e.,* Trust & Safety functions historically have been developed inside individual companies, using in-house proprietary technologies and with little in the way of industry-shared vocabulary, benchmarking, agreed-upon standards, guidelines or external visibility.

33. Although you can read another company's public-facing Terms of Service and Community Guidelines, Trust & Safety program technical and operational functions deliberately aren't visible or obvious to end users, otherwise bad actors could easily evade a platform's protections. Because of this deliberate opacity, individual companies for many years had no choice but to "reinvent the wheel" – on content policy training, moderation and ToS enforcement workflows, trust algorithm and classifier development, escalation processes and public reporting.

34. For example, when I began developing the Adobe Trust & Safety program around 2009, I had no industry organization to turn to, no industry "best practices" documents to cite – nothing to guide my advice to executives and product teams other than my own personal experience developing a similar program at my previous company. My ability to benchmark other companies' practices depended entirely on my own personal network of friends and former work colleagues who, like me, had left Yahoo! to go work at other large tech companies. Without those collaborative relationships, I would have been entirely in the dark.

35. In 2021, the Digital Trust & Safety Partnership (DTSP) was formed to redress this industry-wide problem.[18] The DTSP is an industry-led, voluntary collaboration among large technology companies focused on sharing and standardizing a broad variety of trust and safety practices — particularly in areas like child safety, age assurance, content moderation, terms enforcement and transparency reporting. Meta, Microsoft, Google, Twitter were among its founding members. DTSP does not impose new requirements or define minimum acceptable conduct or legal obligations. Rather, it shares examples of how mature Trust & Safety

[18] Leading Technology Companies Launch Initiative to Promote a Safer and More Trustworthy Internet - Digital Trust & Safety Partnership (February 18, 2021 press release announcing the launch of the Digital Trust & Safety Partnership, "a first-of-its-kind initiative aimed at promoting a safer and more trustworthy internet.").

organizations approach common industry challenges at scale so that individual companies no longer need to "reinvent the wheel."

36. In September 2023, the DTSP published "Age Assurance Guiding Principles and Best Practices" (attached as Exhibit A).[19]

37. As the document's executive summary acknowledges, "every approach to age assurance presents trade-offs."[20] For example, more accurate methods may depend on the collection of additional or sensitive personal data and thus can be in tension with a service's privacy commitments to users, with a user's desire to speak anonymously, or with data minimization principles. Certain age assurance methods may create inequities among users or unfairly discriminate (for example, requiring a credit card as proof of adult status can unfairly exclude users without credit cards). And certain age assurance methods may not be economically feasible for smaller companies or app developers. Hence, there is no one-size-fits all solution.[21]

1. Overview of DTSP Guiding Principles

38. DTSP's age assurance best practices are organized around five guiding principles:

- Safety By Design Proportionate To Youth Risk: Identify, evaluate, and adjust for risks to youth to inform proportionate age assurance methods, as part of implementing safety-by-design.

- Data Minimization/Privacy Protective-Focus: Account for risks to user privacy and data protection as part of development, implementation, and ongoing assessment of age assurance approaches.

[19] Meta is a founding member of DTSP and helped draft these principles. Other members include Google, Apple, TikTok, Microsoft, Snap, LinkedIn and Reddit. *See, About Us*, Digital Trust & Safety Partnership ("DTSP") (listing DTSP's "partners"), https://dtspartnership.org/#aboutus.

[20] *Age Assurance: Guiding Principles and Best Practices*, DTSP, 2 (September 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

[21] *Id.*

- Inclusivity & Equity: Ensure assurance approaches are broadly inclusive and accessible to all users, regardless of age, socioeconomic status, race, or other characteristics.

- Layered Investigation/Enforcement: Conduct layered enforcement operations to implement age assurance approaches.

- Transparency: Ensure that relevant age assurance policies and practices are transparent to the public, and report periodically to the public and other stakeholders regarding actions taken.

39. DTSP emphasizes repeatedly that there is no one-size-fits-all "best practice" solution and that different platforms may reasonably make different design choices while still aligning with industry best practices.[22]

2. DTSP "Layered Enforcement"

40. DTSP defines "layered enforcement" as using multiple, independent age indicators, each of which either corroborates or escalates concerns about user age. No single method is expected to work alone; strength comes from combining some (or all) of them.

41. DTSP examples of layered enforcement practices include:

- Ensuring a neutral self-declared age gate at registration.

- Deploying an age assurance check if a user changes their self-declared age from one that was <18 to an age >18.

- Analyzing user behavior or signals for indicia that the user is under the allowed platform age (for example, on a social media platform that bars users under 13, a "Happy 11th Birthday!" message posted to a user's timeline).

- Training enforcement teams who review age verification escalations using reliable methods for verifying a misreported age (for example, by evaluating appearance or

[22] *See id.* at p. 14.

other signals indicating a younger age) and in appropriate methods for age assurance investigation follow up.

- Allow users to report other users who may have misreported their age.
- Implement technical measures that can help prevent users who have failed an age assurance test from circumventing controls (*e.g.*, by dropping a cookie that prevents a user from starting the process over again via a new registration).
- Potentially offering family accounts or parental verification where a young person's account may be attached to a parental account.[23]

IV. NIST AND IEEE ENGINEERING STANDARDS ARE NEITHER RELEVANT NOR AN ACCEPTED MEASURE OF U.S. AGE GATING BEST PRACTICES

42. When assessing Meta's practices, Dr. McDaniel completely ignores FTC guidance and industry-accepted principles that have guided U.S. age-gating development for more than two decades.[24] Entire sections of his report are dedicated to faulting Meta for allowing "self-declared age" at registration,[25] without once mentioning that (1) the FTC staff FAQs explicitly approve this practice; and (2) it is standard practice within the industry to do so.

43. Dr. McDaniel dedicates other sections of his report to various studies "proving" that users under the age of 13 are on both Facebook and Instagram.[26] He never mentions that FTC staff guidance (1) fully anticipates that young users may lie and (2) states that this type of general knowledge in and of itself gives rise to no specific investigative duty. He likewise doesn't mention that every large social media platform and internet platform in the U.S. faces this exact same challenge and addresses it using the same industry-accepted layered "best practices" that Meta does.

---

[23] *Id. at* p. 14-15.

[24] There are only two brief mentions of "COPPA" in Dr. McDaniel's 300+ page report, neither of which details its requirements or examines them in the context of Meta's practices. *See* Corrected Trial Report of Patrick McDaniel, ¶¶ 47 & 115 (Dec. 15, 2025).

[25] For example, Dr. McDaniel cites studies that reveal what all platforms, the FTC and the vast majority of the general public already know: *i.e.,* that Meta allows self-declared age entry at account creation without requiring proof that the registrant is over 13 (just like every other large US provider). *See* Corrected Trial Report of Patrick McDaniel, ¶ 78.

[26] *See, e.g.,* Corrected Trial Report of Patrick McDaniel, ¶¶ 79-82.

44. Instead, Dr. McDaniel spends much of his report explaining a variety of NIST and IEEE engineering standards then opining that Meta's practices "fail" to meet those standards. Yet NIST and IEEE engineering standards are not in any way relevant here, for the reasons explained below.

A. NIST Engineering Standards Are Only Binding On Federal Government Agencies

45. NIST is a U.S. government body that was established by Congress in 1901 to advance measurement science, standards, and technology to improve U.S. competitiveness. It is now part of the U.S. Department of Commerce.[27] In 2002, Congress enacted the Federal Information Security Management Act (FISMA) to, among other things, ensure the security of government data by mandating that federal agencies adhere to a uniform set of data security standards developed by NIST.[28] Under FISMA, standards developed by NIST are "compulsory and binding" on all federal agencies.[29]

46. FISMA does not in any way extend the binding nature of NIST standards from federal agencies to private industry. Neither does any other U.S. law or regulation or industry "best practice."

47. For this reason, in-house practitioners who develop and oversee day-to-day age-gating programs and related investigations for U.S.-based platforms ***do not look to NIST standards for program requirements.*** IAPP trainings about age-gating do not reference NIST standards. Likewise, there is not a single reference to NIST standards in the DTSP age assurance best practices document.

48. In my role as the executive responsible for ensuring my company's age gating and registration systems met applicable rules and best practices, I have conducted many dozens of in-house training sessions for engineers, product managers, content moderation teams and privacy program managers on the topic of age gating development and enforcement. In more than a

---

[27] *See About NIST,* https://www.nist.gov/about-nist.
[28] *See* Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3553(a)(1)*.; see also* Wikipedia, *Federal Information Security Management Act of 2002* (https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002).
[29] FISMA, 44 U.S.C. § 3553(b)(2)(A).

decade of doing so, I do not recall ever mentioning NIST standards, except for in the following contexts: (1) advising Adobe's government sales team on additional compliance requirements unique to government sales programs and (2) helping the Adobe Compliance team incorporate NIST obligations to government agencies into its Common Controls Framework.[30] Based on my experience in this field, NIST standards are not ever used as an industry benchmark for the design or day-to-day operation of social media age assurance programs.

B. In 2025, The FTC Considered Whether To Make NIST Privacy Standards Mandatory And Expressly Declined To Do So

49. The FTC expressly considered earlier this year whether it should make NIST Privacy Standards mandatory for U.S. based platform operators by using them to define "reasonable" operator behavior when it comes to securing children's data. **It expressly declined to do so.** This occurred in the context of the FTC's 2025 amendments to the COPPA Rule (the first amendments the Commission has issued since June 2013).

50. In a sixty-six page, single-spaced, document published in the Federal Register on April 22, 2025, the FTC explained each of its final rule COPPA Rule amendments in depth, including why it chose to adopt certain amendments and rejected others proposed during the public comment period. These amendments, which became effective on June 23, 2025, included one new definition, modifications to several others, and updates to key provisions to respond to changes in technology and online practices.[31]

51. NIST Privacy Standards came up during a discussion of an amendment to Section 312.8 of the COPPA Rule, which requires operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children" and to "take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the information's confidentiality,

[30] *See* Adobe Common Controls Framework at https://www.adobe.com/trust/compliance/adobe-ccf.html.
[31] *See Children's Online Privacy Protection Rule,* Federal Register / Vol. 90, No. 76 / Tuesday, April 22, 2025 / Rules and Regulations, available at https://www.ftc.gov/legal-library/browse/federal-register-notices/16-cfr-part-312-coppa-final-rule-amendments at 16918.

security, and integrity and provide assurances that they will do so."[32] The FTC amended Section 312.8 to require operators to obtain such assurances in writing.[33]

52. In the Federal Register, the FTC explained that one commenter had urged it to go further than it had, urging adoption of the NIST Privacy Standard as the COPPA Rule definition of "reasonable procedures" – much like an "approved and preferred industry standard" or "Safe Harbor framework." [34] The FTC explained why it expressly declined to do so:

> "[*T]he Commission believes that proposed §312.8(b) properly recognizes that variations in the sensitivity of the personal information operators collect from children and in operators' size, complexity, and nature and scope of activities are important considerations that inform the specific safeguards the Rule should require operators to implement" … and provide(s) operators appropriate flexibility*."[35]

53. Thus, the FTC definitively confirmed that compliance with NIST Standards is not mandated by COPPA – either before the recent 2025 amendments or thereafter. Instead, platforms retain "appropriate flexibility" to decide what procedures are "reasonable" given the facts at hand and the sensitivity of the personal information in question.[36]

54. Even though privacy professionals, Trust & Safety professionals and the FTC all agree that NIST standards aren't relevant to commercial platform age-gating, Dr. McDaniel nonetheless repeatedly invokes them. His report details at length NIST standards on user

---

[32] *Id.* at 16960.
[33] *Id.* at p.16960-62.
[34] *Id. at* 16960 n. 547.
[35] *Id.* at 16960-61.
[36] Notably, NIST is mentioned by the FTC just twice in this lengthy and highly detailed document. In addition to the discussion rejecting making NIST standards mandatory, the FTC mentions NIST in two footnotes explaining why it expanded the definition of "personal information" to include ''[a] biometric identifier that can be used for the automated or semi-automated recognition of an individual, including fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data.'' This amendment occurred, at least in part, because NIST determined that technologies like facial recognition had become substantially more effective. *Id.,* at n. 72, and again at ftn.119.

account data governance,[37] data deletion,[38] age estimation,[39] audit logging,[40] demographic bias characteristics and identity proofing standards,[41] the completeness of data deletion,[42] digital identity guidelines and risks posed by synthetic content,[43] and cryptographic erasure.[44] He then opines that Meta's practices are "substandard" or "fall outside accepted security practice" because he says they fall short of what NIST requires.[45]

55. But because NIST is not applicable to social media company age assurance systems, Dr. McDaniel's opinion is both misleading and irrelevant. Meta is not a federal agency. It does not sell services to federal agencies. No tech company that provides services to the public at large looks to NIST standards when developing or administering its age assurance program. Therefore, NIST standards are not a valid measure of any U.S. company's age assurance controls or practices.

C. IEEE Standards Were Developed For Foreign Nations Like the UK, Australia and Indonesia That Have Adopted Age Verification Laws

56. The IEEE Standards against which Dr. McDaniel evaluates Meta's practices likewise are irrelevant – albeit for a different reason.

57. The Institute of Electrical and Electronics Engineers (IEEE) is a global engineering organization that develops voluntary technical standards across a wide range of disciplines.[46] Its age-assurance initiatives — including IEEE 2089 ("Age Appropriate Digital Services Framework") and IEEE 2089.1 ("Age Assurance Systems") — were drafted specifically in

---

[37] McDaniel Report at paragraph 51 *("Data governance for user accounts encompasses how that data is collected, classified, stored, accessed, retained, shared, and ultimately deleted. U.S. federal standards such as NIST 800-5364 require that access to such data be limited to authorized personnel and systems under clearly defined controls (e.g., NIST SP 800-53 Access Control family). These standards also emphasize the importance of accountability mechanisms, such as audit logging, for actions taken on user accounts.")*

[38] *Id.* at P. 52 ("*NIST 800-8865 establishes the expectation that data deletion must be complete, timely, and irreversible once the data is no longer needed for legitimate operational or legal purposes.")*

[39] *Id.* at p. 71-72.

[40] *Id.* at p. 73 and n. 91.

[41] *Id.* at 72.

[42] *Id.* at 74 ("*When user ineligibility is determined, U.S. federal standards such as NIST SP 800-88 and 800-53 require that personal data be deleted completely, promptly, and irreversibly once it is no longer needed for legitimate operational or legal purposes.").*

[43] *Id.* at 334.

[44] *Id.* at 363.

[45] Indeed, there are a whopping 140 references to NIST in the McDaniel Report and its various exhibits.

[46] *See generally,* https://www.ieee.org/

response to the adoption (or imminent adoption) of age verification laws in jurisdictions like the UK, Australia and Indonesia.[47]

58. All IEEE 2089 and 2089.1 do is provide an engineering perspective on what platforms operating in foreign jurisdictions where age verification is now (or may soon become) the law of the land *might* consider doing when it is time to comply. Accordingly, they are not a relevant measure of what U.S. platforms – where age verification is *not* mandated -- must do for U.S. audiences.

59. I am aware of no general or mixed-use audience U.S. platform that has implemented IEEE 2089-style verification at user registration. And, to my knowledge, no U.S.-based practitioner responsible for age gating compliance or program management considers knowledge of IEEE standards pertinent to their work or to the training materials they develop for their staff.

V. META'S AGE ASSURANCE PRACTICES MEET OR EXCEED INDUSTRY BEST PRACTICES

60. As explained above, experienced privacy and Trust & Safety practitioners look to two primary sources of guidance when developing, operating or evaluating the efficacy of their age assurance program. An age assurance program *must* do what is expressly required by the FTC COPPA FAQ. But a responsible program also *should* voluntarily ensure that it meets "best practices" adopted by companies of a similar size and type in the industry. Experienced practitioners consider their age assurance program responsible and mature if it does both.

61. The very definition of meeting "best practices (whether in legal contracts, NIST cybersecurity guidelines or the dictionary) ***is adhering to practices that have been widely adopted in a particular industry because those practices yield effective results at scale***.[48]

---

[47] *See, e.g., "IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children"* https://5rightsfoundation.com/wp-content/uploads/2024/09/2089-2021-with-disclaimer.pdf 5Rights is a London-based NGO whose work underpins the **UK Age-Appropriate Design Code**. https://5rightsfoundation.com/united-kingdom/. *See also,* IAPP *"Children's Privacy Laws and Freedom of Expression: Lessons from the UK Age-Appropriate Design Code"* (Nov 13, 2023) *https://iapp.org/news/a/childrens-privacy-laws-and-freedom-of-expression-lessons-from-the-uk-age-appropriate-design-code* ("*The safety-by-design principles in the U.K.'s AADC … is complemented by the work the IEEE is doing to develop the 2089-2021 – Standard for Age Appropriate Digital Services Framework.")*.

[48] *See Best Practice, Computer Security Resource Center,* https://csrc.nist.gov/glossary/term/best_practice; *Best Practice, Merriam Webster, https://www.merriam-webster.com/dictionary/best%20practice.*

When it comes to age assurance, the clearest articulation of widely accepted "best practices" is set forth in the DTSP Age Assurance Best Practices document endorsed by a broad swath of U.S. Industry – including Google, Apple, Microsoft, Linked In, Pinterest, Discord, Reddit, Snap, TikTok and others.[49]

62. Dr. McDaniel seems to fundamentally misunderstand what "best practices" are and why they matter. His report *references* the DTSP Age Assurance Best Practices.[50] However, rather than measure Meta's practices against them he, instead, criticizes Meta for testing—and ultimately deciding not to deploy—a variety of additional features that go well above and beyond those best practices. On that basis, he concludes that Meta's efforts are "inadequate" because they do not reflect the outer limits of what is "technically feasible."[51]

63. In Trust & Safety practice, however, "technical feasibility" is not an accepted benchmark or standard for evaluating the adequacy of an age assurance (or any other) program. Companies are not obligated to implement every measure that is "technically feasible" without regard for whether that measure also yields effective results at scale.[52] To the contrary, responsible Trust & Safety programs routinely test, evaluate, and adopt (or reject) potential features based on policy tradeoffs, abuse risk, scalability, and operational impact. The measures that ultimately are proven to work at scale are adopted and, once widely so, become industry "best practices."

64. Based on my review of Meta's public-facing documentation and relevant discovery materials in this case, it is my professional opinion that Meta's age assurance practices meet or exceed *actual* U.S. industry best practices and standards.

---

[49] *See* https://dtspartnership.org/#aboutus.
[50] McDaniel Report ¶ 70.
[51] McDaniel Report ¶ 141.
[52] McDaniel's "technical feasibility" critiques fail to account for real-world operational considerations. For example, he faults Meta for not implementing a Shortened Underage Reporting Flow (SURF) that would have enabled one-click reporting of underage users. *Id*. at ¶ 147. But, as reflected in discovery materials, the under-13 reporting feature is frequently abused and has been used millions of times to target and harass adult users, including political entities, countries, public officials, and celebrities (e.g., mass false reports directed at the Israeli Defense Forces, Kim Kardashian, Emmanuel Macron, and others). See META3047MDL-208-00003249. In that context, a frictionless, one-click reporting mechanism would more predictably increase abusive reporting volume than meaningfully improve the detection of underage users—an outcome that experienced Trust & Safety practitioners would recognize as counterproductive.

A. Meta Follows Long-Accepted FTC Guidance To Businesses On Age Gating

65. Both Facebook and Instagram have industry standard age-gating mechanisms at registration.[53] Both Instagram and Facebook present a neutrally structured birth-date field at sign-up, consistent with the FTC's explicit guidance.[54] Neither Facebook nor Instagram's age gates nudge users toward entering an age over 13, default to a compliant age or discourage truthful entry by warning that younger users will be excluded from certain features.[55]

66. Both platforms likewise have well-defined processes followed by trained staff for investigating any circumstance where Meta obtains actual knowledge that a specific user is under the age of 13.[56]

B. Meta's Age Gating Program Fully Comports With DTSP Age Assurance Best Practices

67. Meta also takes an appropriately layered approach to age assurance for Facebook and Instagram, consistent with the DTSP age assurance best practices.

68. Meta's layered practices include:

- Deploying technical methods to help prevent users who have failed an age assurance test and been deemed ineligible from circumventing the controls.[57]

[53] In addition to relying on discovery materials, I independently reviewed and tested Instagram and Facebook's registration age-gates on December 9, 2025 and compared them, that same day, to those operated by TikTok, Google, X, Microsoft, Adobe and Snap.
[54] *See, e.g.*, Corrected McDaniel Report ¶ 104 (Table 1).
[55] *See, e.g.,* META3047MDL-190-00000002, *et. seq.*
[56] *See., e.g.,* META304 7MDL-012-00000003 (Meta trains thousands of human reviewers to review accounts that are reported by other users for potentially violating the Meta terms of service and content guidelines. In the course of reviewing these accounts in response to any type of report, a reviewer may notice certain details suggesting that the account holder may be a child under 13 (e.g., photos posted to the account reflecting age or text in the account bio stating an age under 13), in which case the reviewer will escalate the account for underage review. Meta may also identify underage users through other review processes including, for example, where Meta requires users to provide identification to access certain features (e.g., Meta Verified)). *See also* META3047MDL-146-00072824 (overview of age assurance workflows) and Allison Hartnett Deposition at p. 182 *et seq.*
[57] *See., e.g., META3047MDL-019-00129336* (describing 12 hour cooling off period to prevent additional registration attempts when user enters date of birth under 13) and META3047MDL-053-00012657 at 12662 (If a user tries to put in a U13 birthday, "After two consecutive attempts, the user will be prevented from creating an account and locked out of the registration process for a period of 12 hours.")

- Employing machine-learning classifiers trained on reliable signals for predicting whether an account belongs to someone over or under the age of 18.[58]
- Directing accounts flagged as potentially underage through an automated process that determines whether the account should be escalated for human review or immediately actioned.[59]
- Where classifiers are not confident in their prediction, flagging such accounts and escalating them for review by human moderators trained in investigating account age.[60]
- Suspending accounts that have been checkpointed so that they are no longer accessible to the user or visible to other users during the evaluation process.[61]
- Closing accounts that fail an age checkpoint and, once the period for user appeal has expired, erasing their data. Moreover, any accounts linked to the failed account in Meta's Account Center (for example, a Facebook account linked to an Instagram account) are likewise closed and deleted.[62]

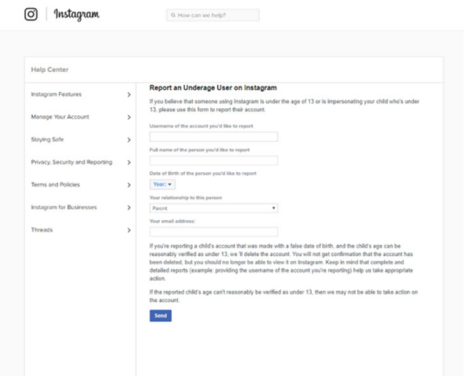


Figure 2 - Instagram "Report an Underage User" Screen META3047MDL-040-00000322. See also META3047MDL-208-00003307 for Facebook form.

[58] *See* META3047MDL-012-00000005 *et seq.*; META3047MDL-146-00072880 (high-level overview of the age labels used for training and evaluating the age prediction models); Allison Hartnett Deposition at p. 175 *et. seq.*

[59] META3047MDL-012-00000003 *et. seq.* (Meta may learn that a user is underage directly from the user, if the user attempts to change the date of birth on their account to a date that would make them under 13. As of February 2021, the user will be automatically placed in an age checkpoint and must provide sufficient proof that they are old enough (i.e., 13 or over in the United States) to use Instagram before they will be permitted to continue to use the service.)

[60] *See* META304 7MDL-012-00000001 at -0006-0008 (All potentially underage accounts that are manually reviewed are reviewed using Meta's content review platform, which is specifically designed for large-scale manual review efforts. The platform standardizes the underage review process and allows Meta to track and properly document decisions made. To ensure that the human review process is consistent and that reviewers evaluate each profile using the proper criteria, Meta's content review platform provides
reviewers with a 'decision tree' or standardized flow that they must follow for each flagged account. Reviewers are also able to include notes and provide additional context for why they made a particular decision.)

[61] *See* META3047MDL-012-00000007.

[62] *See* META3047MDL-012-00000010.

- Deploying an age assurance check via a third-party vendor if a user changes their self-declared age from one that was under 18 to an age over 18.[63]
- Automatically checkpointing accounts if users change their self-declared age from one that was 13 or older to an age under 13.[64]
- Allowing users (and non-users) to report directly to Meta that a particular user is under the age of 13.[65]
- Implementing "Teen Accounts" on both Instagram and Facebook, which default to protective settings and offer parents access to controls like approving changes to teen settings or permissions, monitoring usage, setting time limits and more.[66]

69. In my experience, this is everything I would expect a mature, responsible U.S.-based internet or social media company's age assurance program to do — and more. Based upon my review and my professional experience, I am confident that Meta's program is at least comparable to (and in many instances likely exceeds) age assurance programs operated by DTSP members of similar size.

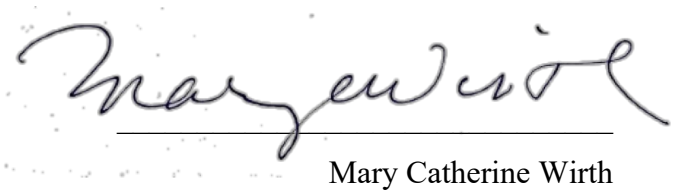
[63] *See* META3047MDL-012-00000015 (When a user attempts to change their date of birth from an age under 18 years old to an age 18 years or older, Meta provides the user multiple options for verifying age, including the option to upload a self-portrait video. If a user elects this option, Meta will collect a video selfie from the user and share a selfie image with third-party service provider, Yoti, a leading age verification provider for several industries around the world, including social media, gaming, and age restricted ecommerce. Yoti's technology will estimate a user's age based on their facial features, and will share back to Meta the user's estimated age. Meta and Yoti delete the uploaded image after Yoti sends Meta the user's estimated age, and the video selfie is not used for any other purpose other than to verify the user's age. If Yoti estimates that the user is under the age of 13, the user will be placed in an age checkpoint.). *See also* Letter from Meta to Richard Durbin (Apr. 19, 2024*)* https://www.judiciary.senate.gov/imo/media/doc/2024-01-31-qfr_responses-zuckerberg1.pdf.

[64] *See* META3047MDL-053-00012657 at 12664-65 (When a user changes their date of birth from an age 13 or older to an age under 13, their account is automatically placed in a checkpoint on both Instagram and Facebook, and the user is required to prove their age within the specified period to regain access to their account).

[65] *See, e.g.,* META3047MDL-012-00000002, *et. seq.* (Since at least January 1, 2019, anyone, including individuals who do not have an Instagram account, can report to Meta that a user is or appears to be under the age of 13 by filling out an online reporting form.); META3047MDL-053-00012709 at 12716 ("Anyone, including individuals who do not have a Facebook or Instagram account, can report to Meta that a user is or appears to be under the age of 13 by filling out a platform-specific online reporting form.").

[66] *See, e.g.,* Meta Family Center (https://familycenter.meta.com/).

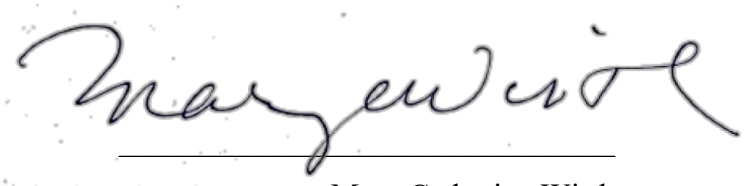
Executed on January 9, 2026.



Mary Catherine Wirth

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.

January 9, 2026



Mary Catherine Wirth

Exhibit A

Digital Trust
& Safety Partnership

Age Assurance

Guiding Principles and Best Practices

September 2023

Digital Trust
& Safety Partnership

Table of Contents

Digital Trust & Safety Partnership

Executive Summary

Digital services work to design safe, age-appropriate experiences, including by implementing "age assurance" practices to establish a user's age.

A variety of age assurance approaches exist, including age verification based on review of identity documents or parental consent; age estimation based on inferences made from user data, physical characteristics, or other measures; and self-declaration by the user.

Every approach to age assurance presents trade-offs. Key challenges include the fact that more accurate methods may depend on collection of new personal data, and thus can be in tension with a service's privacy commitments to users and legal obligations. Methods may also create inequities among users, unfairly discriminating against certain people, and may not be economically feasible for smaller companies.

There is no one-size-fits all solution in this area. Instead, different services opt for different approaches based on a variety of factors, including but not limited to users of the service, type of service offered, risk calculation, privacy expectations, and economic feasibility.

As part of the Digital Trust & Safety Partnership's practicing companies' commitment to its overarching Trust & Safety Best Practices Framework, this document describes a range of current best practices for age assurance.[1] We identify five guiding principles and then note how companies have used these principles to develop example best practices for age assurance. Of course, the specific practices that services use may vary by digital product or feature and evolve with both the challenges faced and advances made in age assurance technologies.

The five guiding principles are:

1. Identify, evaluate and adjust for risks to youth to inform proportionate age assurance methods, as part of implementing safety-by-design.
2. Account for risks to user privacy and data protection as part of development, implementation, and ongoing assessment of age assurance approaches.
3. Ensure assurance approaches are broadly inclusive and accessible to all users, regardless of age, socioeconomic status, race, or other characteristics.
4. Conduct layered enforcement operations to implement age assurance approaches.
5. Ensure that relevant age assurance policies and practices are transparent to the public, and report periodically to the public and other stakeholders regarding actions taken.

[1] This publication was developed by the DTSP Working Group on Age-Related Practices, facilitated by Betsy Masiello and Derek Slater of Proteus Strategies.

Digital Trust & Safety Partnership

Introduction

Young people[2] increasingly rely on digital services in every aspect of their lives, from educational experiences to social interactions with friends, to engagement with entertainment, games, news and other information, and much more. They also move across and through these services fluidly. Digital services work to design age-appropriate experiences, including by designing specific unique content experiences and safety features. Developing digital services that align with the age of individual users poses various challenges. These challenges include (but are not limited to) the complexity in defining age-appropriate content across culturally diverse communities across the world, accounting for the role of the parent in a teen's life, and the inherent tension in accurately determining a user's age while also respecting privacy. There is also a lack of clear universally agreed upon standards upon which to gauge a service's efforts, although efforts to create such standards are ongoing.[3] The practices delineated herein concentrate specifically on principled strategies to assure a user's age with sufficient accuracy ("age assurance") amidst the myriad difficulties associated with this particular objective. It does not address other aspects of delivering age appropriate experiences.

While digital services and all relevant stakeholders have aligned around the need to offer age appropriate experiences, they have not aligned on a solution that works for all services. A variety of age assurance approaches exist at present, and every approach presents trade-offs. Enhancing confidence in users' age carries implications for safeguarding their privacy rights, ensuring their access to information, and preserving their freedom to engage in digital experiences without constraints. These implications hold significance not only for young individuals but for all users of the service. Moreover, the risks associated with youth accessing the service will vary depending on its nature. For instance, a service may be for adults-only, youth-directed, or purpose-built for a mixed audience; services might involve public or private interactions with third parties, or focus instead on engagement with particular types of content. Each service's risk profile will vary, as do the expectations of its users based on the principles, values, and features of the service. Additionally, different age groups (such as teens) move fluidly across varying services. All of this requires careful consultation with different stakeholders, including with youth themselves, to develop best practices.

To help define an overall framework for what constitutes responsible approaches for digital services, the Digital Trust & Safety Partnership (DTSP) has developed a flexible set of best practices arising from its Trust & Safety Best Practices Framework. As part of fulfilling the Commitments in the Best Practices Framework document, some services may employ age assurance practices as part of an overall approach to addressing risks to young users and developing age appropriate experiences.

---

[2] There is no standard definition of young person, youth, child, teenager or adult when discussing age appropriate experiences online. For the purposes of this report, we will rely on the terms "youth" or "young user" and "adult" throughout this paper to represent a general bifurcation between "of-age" and "underage" users, noting that the specific determinant age will vary by jurisdiction around the world. As with the UN Convention on the Rights of the Child, we intend here to refer to "means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier," although services certainly make further delineations based on on a range of factors, including local law.

[3] See, e.g., https://www.iso.org/standard/80399.html

Digital Trust
& Safety Partnership

In this document, we outline the challenges service providers face in age assurance, and then highlight age assurance practices online. We identify five relevant guiding principles for developing and deploying best practices, and then share specific practices for how the framework may be put into action. Of course, the specific practices that services use may vary by digital product or feature and will evolve with both the challenges faced and advances made in age assurance technologies.

While we limit our focus here to age assurance, it is important to recognize that it is only one part of how services may address the challenge of building age appropriate experiences online.

Digital Trust
& Safety Partnership

Age Assurance Methods

There are a wide range of practices deployed to gain confidence in a user's age, and an accompanying range of language used to describe them. Age assurance is typically an umbrella term used to describe the full range of practices that services deploy to establish, determine, or confirm a user's age with some level of confidence. These methods may be used by themselves or in combination with one another within a given service.

Age Verification

At one end of the age assurance spectrum, there are a number of methods to verify a user's age that rely on a trusted authority. In these cases, digital service providers rely on third-party, authoritative credentials, or more recently, a government Application Programming Interface (API) to get confidence of a user's age; alternatively, providers rely on parental[4] consent. All of these methods have limitations and drawbacks that must be taken into consideration when balancing against the benefit of having a highly trusted third party confirm a user's age.

Identity document verification is a mechanism for gathering age information and credentials. It requires access to third-party documentation, typically government-issued IDs or other forms of documentation that otherwise verify an individual's age.[5] In the context of age verification, service providers typically retain only the information related to the person's age while discarding the actual identity documents provided. Nonetheless, the user must provide more information than what is needed to share their age. Digital service providers aim to address privacy concerns by minimizing the retention of sensitive personal information. In addition to these challenges, identity document verification can present equity challenges as access to government IDs or other necessary documentation to verify their age and identity, such as birth certificates, varies across socioeconomic backgrounds. In some cases, the social or political context makes it risky for certain users to obtain or carry identity documentation.

Implementing identity verification in-house is a significant operational challenge, and presents trade-offs. Much like other trust and safety functions, identity verification requires a combination of machine learning techniques and human review in order to detect fraudulent attempts at verifying an identity and age, and to provide users with adequate appeals processes. In addition to the operational complexity of implementing these reviews, collection of this additional identity data raises issues related to privacy and data protection.

There are a number of third-party vendors that offer identity-verification-as-a-service, which reduces the operational overhead for a digital service provider to stand up their own verification workflow, but still represents an added cost and may also create an opacity around data practices that is challenging for digital service providers to navigate.

---

[4] For purposes of this paper, we intend "parent" to refer broadly to the legal guardian of the young user.

[5] Documentation that might be accepted in an identity verification process may include, for example, a birth certificate, school IDs, utility bills in the individual's name, bank account or credit card verification, or real estate ownership documentation.

Digital Trust
& Safety Partnership

More recently, some governments are deploying ID systems[6] that, in turn, support identity verification. Governments have been successful in common standards for Machine Readable Travel Documents[7] and an equivalent effort could be made to establish a common format for digital government IDs for use online.

For businesses, these may reduce operational overhead, although that depends greatly on precisely how they're implemented; for instance, if every government develops its own approach rather than relying on a common standard, then it will still be cumbersome for many services to use different digital IDs in a consistent manner. Moreover, reliance on government ID systems necessarily raises concerns around government collection of data and monitoring of user's daily lives online.

Parental consent is a method relying on validation from a parent (or legal guardian) and is in some cases required in existing regulations. Some regulators have relied on parental consent when mandating digital service providers verify that a user is "of-age" to access a given service. For instance, the Children's Online Privacy Protection Act (COPPA) in the United States requires that services get parental consent if they know that a user is under the age of 13. COPPA has had the effect of bifurcating services into those that are directed at youth under 13 and implement parental consent, and those that do not allow users under 13. Similar rules exist in other jurisdictions when it comes to collection and analysis of personal data, albeit with varying ages of consent. For instance, in Europe, the General Data Protection Regulation's (GDPR) Article 8 allows member states to set the age between 13 to 16; Australia's guidelines presume that anyone under 15 does not have capacity to consent; and, in Korea, data privacy law sets the age at 14. Age of consent is also under active debate in many jurisdictions.

When parental consent can be obtained, it provides some assurance that the child's parents are comfortable with the child accessing a given service or feature. Parental consent can be an important tool for involving parents in a young user's online experience, but it does not guarantee that user is the required minimum age, nor does it offer service providers knowledge of the child's actual age. At best it offers the parent an opportunity to provide the user's stated age, rather than the user doing it themselves. Parental consent also comes with the burden of verifying parental responsibility and the relationship between two user accounts; it may be possible to verify one account holder is an adult with a credit card, for example, but that may not verify in any reliable way that the second account is that adult's child. Furthermore, some youth lack parents who can be relied upon to provide verification of the user's age and parents may verify age inaccurately. The Irish Data Protection Commissioner has noted that "there aren't yet many ways of checking parental consent which are accurate, proportionate and that actually work in practice."[8]

---

[6] For example, the European Union is developing a European Digital Identify, see https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en; a number of US states have either implemented or are in the process of developing digital IDs or or otherwise add a state ID card to a mobile device - see e.g., Colorado's existing digital ID program at https://mycolorado.state.co.us/ and California's in-development digital ID at https://cdt.ca.gov/digitalid/

[7] See https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[8] See https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_ParentalConsent.pdf

Digital Trust
& Safety Partnership

Age Estimation

As part of a comprehensive risk management system, digital service providers sometimes deploy age estimation techniques to mitigate the risk of underage users gaining access to inappropriate content or experiences. These techniques do not verify a user's age, but rather provide the service provider with some degree of confidence that a user is above or below a given age, based on assessment of some inherent features or behaviors of the user. These techniques may be used on top of asking for age or verifying age via documentation.

Capacity testing is a method that deploys a test to determine a user's capacity for knowledge or analytical thought as a proxy for age. For example, a user may be asked to solve a puzzle or complete a math test. While capacity testing requires very little data to be collected about a user, it has limitations. As a practical matter, it can lack precision, making it unhelpful in determining age-appropriateness except in the most general of senses. It also can generate inequitable outcomes based on users' exposure to educational opportunities and developmental age. Finally, it becomes increasingly ineffective at differentiating ages as a person grows older and gains greater literacy and overall capacity, and users may circumvent the tool by, for instance, getting help from another person.

Age inference is a more advanced estimation method that analyzes data related to a user in order to estimate a user's age. This technique can be deployed on data that is already collected by a digital service provider as a function of using the service. While the data may be produced by the user's interaction with the service itself, it's also possible to incorporate data collected through other services operated by a given provider or third-party sources.

For example, a social networking site may evaluate behavioral signals based on how a user engages with the service, or a media platform may evaluate signals based on the type of content a user is consuming. If a user seeks to consume mostly youth-directed cartoons, then a service might infer that they are a young user themselves; by contrast, if a user primarily seeks out topics like mortgage information, then a service might infer that they are an adult. In turn, if it has a certain level of confidence that the user is young, a service might then prompt the user to produce other evidence of their age; similarly if a user appears to be posing as a young person to gain access to other young users, a service might also prompt the user to produce other evidence of their age.

Because it is necessarily dependent on signals collected during use of a digital service, age inference is a technique that cannot easily be deployed upon account creation. Instead, it is typically deployed as part of a broader age assurance program that incorporates multiple methods, which may be built and operated in-house or by third-party vendors.

Though inference may not depend on additional data collection (at least prior to prompting for further information), it can still raise privacy and data protection concerns. For instance, use of a user's web browsing history might raise concerns when used to do age assurance on a separate service operated by the same provider.

Digital Trust
& Safety Partnership

Social vouching is the use of a user's social connections to add additional verification layers to a user's age. This technique relies on asking other users, whose ages and/or identities have already been verified with some degree of confidence, to "vouch" for the stated age of a given user.

Physical age estimation is the use of physical characteristics, most notably facial images, to estimate a user's age. This method relies on collection of data at account creation, or during a subsequent age assurance process after a user is suspected of being underage. Typically this data would not otherwise be collected in the provisioning of the service. This additional data collection heightens the associated privacy risks for the user, and demands strict compliance with data protection standards on the part of the service provider or vendor. In part as a result of these trade-offs, age estimation using facial images is a method that has, to date, been most widely deployed by vendors as opposed to built in-house by service providers.

While this form of age estimation can provide a great degree of accuracy in estimating a user's age, there are limitations associated with demanding this additional collection of personal data from users. Some users may be concerned about the additional collection, and use of a specialized age assurance vendor does not necessarily address this concern. In fact, when a vendor is providing the service for the consumer-facing digital service provider, it may be that much more challenging for users to easily understand how their data will be used and protected. Furthermore, there are potential issues to consider with regard to accuracy and bias, including potential racial bias, of physical age estimation techniques.

Self-declaration

Self-declaration (sometimes referred to as "asserted age assurance") is the practice of asking a user to declare their age. Some self-declaration implementations merely ask a user to affirm they are "of age", asking a yes or no question as to whether a user is above a given age; others are considered "neutral" methods that simply ask the user to state their age. This is the most widely deployed method to date of age assurance, but is also highly susceptible to users providing false information. It is often deployed as one method within a broader risk management system; for example, a service might use self-declaration and subsequently deploy a behavioral age estimation method against all users.

Digital Trust
& Safety Partnership

Method Implementation Choices

There are also a range of different ways to implement age assurance methods. For instance:

- **Platforms and devices age assurance**: Some platforms and device manufacturers may implement an age assurance method that results in an age for the user which is then made available to apps and other services on the device.
- **Third-party validation**: Third-party validation, in the context of identity verification and age assurance, refers to the involvement of an external entity or service provider to verify and validate the identity or age of an individual. Instead of relying solely on internal processes or self-declaration, organizations use third-party services or systems to independently confirm the accuracy and legitimacy of the information provided by the individual. For instance, a bank, utility, or credit agencies might provide information to a third-party service that the person is a customer and thus is of a given age. This can also take the form of government validation, such as through digital identity programs, as discussed above.
- **Vendor-provided age assurance**: Some services will hire vendors that perform age assurance methods, using proprietary technology or by aggregating data from a variety of sources. A user's personal data is passed to these vendors, who are then responsible for performing the actual age assurance test, as well as implementing data privacy and security practices.
- **In-house services**: Some service providers will implement age assurance methods entirely in-house, using a combination of proprietary technologies, open source software, and operational enforcement mechanisms. A provider may also make these services available to third parties.

Services might rely on a variety of implementations, and may apply different methods in different geographies based on local requirements.

Key Challenges & Trade-Offs

Several challenges emerge in developing age assurance approaches. Key characteristics that digital service providers look to incorporate in developing these approaches include:

- **Effective**: Having confidence that a user is a given age allows a digital service provider to provide them with an age-appropriate experience, in a way that is accurate and hard to circumvent.
- **Accessible, inclusive and equitable**: Age assurance should not result in inequitable outcomes for a given user, and the complexity of processes should not overly burden users in ways that discourage appropriate use of a service.
- **Privacy-preserving and data-protecting**: Protecting a user's privacy, especially a young user's privacy, demands adherence to key privacy principles including data minimization, as well as implementation of security measures to protect data.
- **Affordable**: Implementation costs must be reasonable and proportionate.
- **Risk-appropriate**: The approaches deployed should be proportionate to the risks associated with underage access to a given service, as well as the risks of inaccurate determinations regarding age.

Incorporating each characteristic comes with trade-offs, and there is no one-size-fits-all solution. Highly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID. Some methods that may be economical may have the consequence of creating inequities among the user base. And each service and even feature may present a different risk profile for younger users; for example, features that are designed to facilitate users meeting in real life pose a very different set of risks than services that provide access to different types of content.

Services will face different challenges based on their level of maturity and size, as well as the nature of risks associated with their service. Some age assurance methods may not be economical for smaller companies, and if these methods are not risk-appropriate may thus unduly burden these companies. While larger service providers may find use of these vendors a viable investment to make, particularly if their service is oriented toward higher risk activities, smaller companies may not be able to sustain their business if these costs are imposed. It is therefore important that companies are able to mitigate age-associated risks in different ways, for example by mitigating the risk of youth-centric harms occurring on a service before implementing a costly age verification method.

Similarly, age assurance methods may have tensions with and need to be balanced against a service's privacy commitments to users, which may be entirely appropriate based on the risk profile and purpose of a service. It is important that services retain flexibility to make these decisions for implementing age assurance in the broader context of mitigating age-associated risks, including based on the nature of the service provided.

Instead of a single approach, we acknowledge that appropriate age assurance will vary among services, based on an assessment of the risks and benefits of a given context. A single service may also use different approaches for different aspects or features of the service, taking a multi-layered approach.

The following principles and practices represent how Practicing Companies may put into action age assurance, in the context of a broader trust and safety program and the overall DTSP Best Practices Framework.

Digital Trust
& Safety Partnership

Guiding Principles and Best Practices

Principle 1

Identify, evaluate and adjust for risks to youth to inform proportionate age assurance methods, as part of implementing safety-by-design.

Aim: Ensure that companies engage in adequate forethought to the specific risks to youth, and incorporate insights into age assurance methods.

Commentary: Practicing Companies care deeply about the development of age-appropriate experiences that both protect the safety and respect the rights and interests of youth, including their rights to express and access information, and their right to privacy.[9]

To develop a proportionate approach for age assurance, Practicing Companies evaluate risks that are specific to youth – for instance, content that may be inappropriate for younger users, or contact from adults for purposes of grooming. Such risks and impacts are evaluated as products and features are developed, and they may evolve over time after a product or feature is launched. In turn, ongoing assessment and evaluation of risks and impacts is critical. They also assess how age assurance methods may impact both youth and other users.

Examples of specific practices to assess and analyze risks to youth when deploying age assurance include:

- Identify and categorize risks to youth related to content, conduct, contact with third parties, and commercial relationships made possible by a product or feature.
- Develop specialized expertise, insight, and analysis capabilities related to high-impact risks to youth and appropriate mitigation measures.
- Develop and implement frameworks and best practices for risk and impact assessment, which take into account, for instance, the likelihood of youth engaging with a service or feature; the audience the service is designed for; the evolving capacities of young people as they age; foreseeable risk; and the best interests of the young people.
- Consult third parties, including youth and families, in assessing risks and impacts, and selecting age assurance methods.
- Include experts in young people and their safety throughout the product development process, and provide for ongoing feedback both pre-launch and post-launch on risks to youth as well as upholding their rights.

[9] See UN Convention on the Rights of the Child, UN Office of the High Commissioner, November 1989; General Comment No. 25 (2021) on children's rights in relation to the digital environment, OHCHR, March 2021.

Digital Trust
& Safety Partnership

Principle 2

Account for risks to user privacy and data protection as part of development, implementation, and ongoing assessment of age assurance approaches.

Aim: Ensure that age assurance approaches respect data protection and privacy rights, including and especially the privacy rights of young people.

Commentary: Privacy and data protection must be taken into account when evaluating what is most appropriate for a given feature or product. Each method of age assurance has different impacts on user privacy, and different services have different baseline privacy practices that impact user expectations. Along with considering how best to respect privacy when implementing age assurance approaches themselves, a particular challenge for digital service providers is gaining insight into and confidence in the privacy practices of third-party age assurance vendors, which is necessary not only to meet their obligations to users but also to meet regulatory and compliance responsibilities appropriately.

Examples of specific practices to protect user privacy rights include:

- Minimize collection of personal data for age assurance, in a manner proportionate to assessed risk, and design tailored practices regarding the retention, deletion, and use of data.
- Use sensitive data collected solely for age assurance only for that purpose, and delete such data expeditiously once a particular method is complete.
- Analyze personal data exclusively on-device wherever possible, to prevent its transmission to servers (including the digital service provider's servers) that are beyond the individual's control.
- Use age estimation methods on data that is already collected as a function of providing the service, to prevent collection of new personal data.
- Implement age assurance through a vendor such that any new personal data that is collected (e.g., a selfie photo) is only sent to the vendor that performs the age assurance test, not first to the digital service provider.
- Require that vendors apply high privacy and security standards, ensure appropriate third-party review and confirmation that those standards are met.
- Provide transparency to end-users about how their data is collected, used, and retained.
- Complete a Data Protection Impact Assessment before implementing any new age assurance method.
- Where possible, rely on interoperable age assurance solutions that minimize the burden on the user to provide additional information to new services, and mitigate the data protection risks the user must bear.

Digital Trust
& Safety Partnership

Principle 3

Ensure assurance approaches are broadly inclusive and accessible to all users, regardless of age, socioeconomic status, race, or other characteristics.

Aim: Ensure age assurance does not unduly impede access to the service, taking into account the disparate impact that age assurance methods may have.

Commentary: Age assurance would be counterproductive if it had the effect of eliminating access to digital services for wide swaths of users for whom those services are appropriate. Deploying an age assurance method that relies on, for example, a government-issued ID may have the effect of discriminating against younger users and users who've had no need to obtain a government-issued ID in their locale. Similarly, certain types of age estimation such as those based on facial images may have greater or lesser confidence levels for populations of a certain ethnicity or age demographic. Practicing Companies take these different effects on inclusivity into account when designing an age assurance approach.

Examples of specific practices to ensure inclusivity and accessibility for all users include:

- To the extent feasible and aligned with legal requirements, select age verification vendors that provide options beyond government-issued IDs, such as birth certificates and school IDs, or a combined unique account identifier and picture of the user, to ensure users without access to government-issued IDs are not discriminated against.
- Provide an accessible, easy-to-navigate appeals mechanism for those users who failed an age estimation test.
- Perform an impact analysis before deploying age estimation techniques to specific populations of users to understand any discriminatory outcomes and mitigate them.
- Provide a process for users to flag that a user is underage, and in concert with an enforcement action give that user in question access to an appeals process to prove their age.
- Conduct reviews of age assurance implementations, including with credentialed third-party vendors or service providers as appropriate.
- Consult with third parties to evaluate the impacts of age assurance methods under consideration.

Digital Trust
& Safety Partnership

Principle 4

Conduct layered enforcement operations to implement age assurance approaches.

Aim: Ensure operational capacity exists to prevent users from accessing services or features that are inappropriate to the level of risk, limit access for those who are discovered to have accessed risk-inappropriate services or features, and to provide an appeals process for users whose access is impacted because of age assurance processes.

Commentary: Services define and train an enforcement function within the company that is equipped to implement policies on age appropriate access based on the output of age assurance methods. Based on evaluations of risks, companies invest in a range of technologies and personnel to both select appropriate methods for age assurance and ensure their enforcement on an ongoing basis. These operations are "layered" in the sense that different approaches may be combined and different approaches may apply to different parts of a service, content, or features, based on levels of risk. Services also reevaluate and adjust these operations based on evolving technologies and best practices.

Examples of specific practices of layered enforcement operations to implement age assurance approaches include:

- Set default limits on access to and discovery of the service, certain features, or particular content, subject to in-product notifications about age appropriateness of that content and/or some other form of age assurance.
- Label and, where appropriate, classify services as appropriate for only certain ages, and coordinate with distribution platforms to apply relevant limits for downloads and access by underage users.
- Deploy an age assurance check if a user changes their self-declared age from one that was <18 to an age >18.
- Analyze behavior on a service for all users who self-declare an appropriate age at account creation, identifying users who may have inputted false information and are underage, and proactively putting these users through an additional age assurance test. Behavior indicative of a self-declaration being inaccurate might be, for example, a message celebrating a user's own 11th birthday or repeated engagement with predominantly youth-directed content.
- Train enforcement teams to identify indicia of a user who has mis-reported their age (for instance, their appearance signals they are actually younger), and a method for triggering further age assurance.
- Allow users to report users who may have mis-reported their age and thus should be limited from the service or certain features.

Digital Trust
& Safety Partnership

- Implement technical methods that can help prevent users who have failed an age assurance test and been deemed ineligible from circumventing the controls (e.g., by immediately signing up with a different account).
- Apply new age assurance tests to existing users as a company improves or changes its assurance processes or makes relevant changes to a product or feature.
- Offer family accounts in connection with parental verification by attaching a young person's account to the parent's.
- Empower users or community moderators to set age requirements for engagement with particular content or communities within a service.

Principle 5

Ensure that relevant age assurance policies and practices are transparent to the public, and report periodically to the public and other stakeholders regarding actions taken.

Aim: Ensure users and the public have insight into a service's age assurance methods.

Commentary: Transparency serves a key function in informing the public and educating various stakeholders about a Practicing Company's age assurance practices, while also building trust over time in the sufficiency of an industry's standard of care. At the same time, transparency needs to be considered alongside the risk of users figuring out how to game age assurance systems.

Examples of specific practices to provide transparency about age assurance practices include:

- Explanations why age or birth date is collected as part of account sign-up.
- Implementation of open source age assurance solutions, such that the implementing code can be easily inspected by external stakeholders and experts.
- Providing third-party researchers access to implementation details and data on age assurance effectiveness such that evaluations of a given method's appropriateness can be made by external actors.
- Publishing data that explains the cost burden of different age assurance methods for providers of varying scale.
- Help center articles explaining a service provider's partnership with an age assurance vendor, including what data is shared and an overview of the vendor's data practices.
- Providing quantitative and qualitative information about enforcement of age assurance policies and practices.

Digital Trust & Safety Partnership

Definitions

For purposes of the DTSP Age-Related Best Practices Framework and the accompanying Commentary, the following definitions apply:

Age Assurance: an umbrella term used to describe the full range of practices that services deploy to gain confidence in a user's likely age, including age verification and age estimation solutions. The word 'assurance' refers to the varying levels of certainty that different solutions offer in establishing an age or age range.

Age Estimation: refers to a range of methods aimed to develop a degree of confidence that a user is above or below a given threshold, in order to allow or deny access to age-restricted online content or services.

Age Verification: measures which determine a person's age to a high level of certainty, usually through relying on third-party documentation or parental consent to verify a user's age.

Commitment: The actions committed to by Practicing Companies to identify and address Content- and Conduct-Related Risk as part of the overall DTSP Best Practices Framework. This document does not include new Commitments, but rather Practices that may be used to implement the overall Commitments.

Content- and Conduct-Related Risk(s): refers to the possibility of certain illegal, dangerous, or otherwise harmful content or behavior, including risks to human rights, which are prohibited by relevant policies and terms of service.

Contact-Related Risk(s): refers to the possibility of illegal, dangerous, or otherwise harmful contact from a third party to a young user, which are prohibited by relevant policies and terms of service.

Commercial Relationship-Risk(s): refers to the possibility of illegal, dangerous or otherwise harmful commercial and contractual relationships or pressures that a young user may experience in using a service.

(References to "**Risks**" shall be understood to refer cumulatively to **Content-**, **Conduct-**, **Contact-**, and **Commercial Relationship-Related Risk(s)**.)

Practicing Companies: Providers of products or services that have adopted the Commitments described in the overall DTSP Best Practices Framework.

Trust and Safety: refers to the field and practices that manage challenges related to Content- and Conduct-Related Risk(s), including but not limited to consideration of safety-by-design, Product Governance, risk assessment, detection, and response, quality assurance, and transparency.

Youth and Young User: For the purposes of this report, we will rely on the terms "youth" or "young user" and "adult" throughout this paper to represent a general bifurcation between "of-age" and "underage" users, noting that the specific determinant age will vary by jurisdiction around the world. As with the UN Convention on the Rights of the Child, we intend here to refer to "means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier," although services certainly make further delineations based on on a range of factors, including local law.

Digital Trust & Safety Partnership

Appendix: Mapping age assurance principles and practices against the DTSP Best Practices Framework

Guiding Principle 1: Identify, evaluate and adjust for risks to youth to inform proportionate age assurance methods, as part of implementing safety-by-design.

Age Assurance Principles and Practices	DTSP Best Practices Framework				
Best Practices	Product Development	Product Governance	Product Enforcement	Product Improvement	Product Transparency
Identify and categorize risks to youth related to content, conduct, contact with third parties, and commercial relationships made possible by a product or feature.	✓			✓	
Develop specialized expertise, insight, and analysis capabilities related to high-impact risks to youth and appropriate mitigation measures.	✓			✓	
Develop and implement frameworks and best practices for risk and impact assessment, which take into account, for instance, the likelihood of youth engaging with a service or feature; the audience the service is designed for; the evolving capacities of young people as they age; foreseeable risk; and the best interests of the young people.	✓			✓	
Consult third parties, including youth and families, in assessing risks and impacts, and selecting age assurance methods.	✓			✓	
Include experts in young people and their safety throughout the product development process, and provide for ongoing feedback both pre-launch and post-launch on risks to youth as well as upholding their rights.	✓			✓	

Digital Trust & Safety Partnership

Guiding Principle 2: Account for risks to user privacy as part of development, implementation, and ongoing assessment of age assurance approaches.

Age Assurance Principles and Practices	DTSP Best Practices Framework				
Best Practices	Product Development	Product Governance	Product Enforcement	Product Improvement	Product Transparency
Minimize collection of personal data for age assurance, in a manner proportionate to assessed risk, and design tailored practices regarding the retention, deletion, and use of data.	✓	✓	✓		
Use sensitive data collected solely for age assurance only for that purpose, and delete such data expeditiously once a particular method is complete.		✓	✓		
Analyze personal data exclusively on-device wherever possible, to prevent its transmission to servers (including the digital service provider's servers) that are beyond the individual's control.		✓	✓		
Use age estimation methods on data that is already collected as a function of providing the service, to prevent collection of new personal data.		✓	✓		
Implement age assurance through a vendor such that any new personal data that is collected (e.g., a selfie photo) is only sent to the vendor that performs the age assurance test, not first to the digital service provider.		✓	✓		
Require that vendors apply high privacy and security standards, ensure appropriate third-party review and confirmation that those standards are met.		✓	✓		
Complete a Data Protection Impact Assessment before implementing any new age assurance method.	✓	✓			
Where possible, rely on interoperable age assurance solutions that minimize the burden on the user to provide additional information to new services, and mitigate the data protection risks the user must bear.		✓	✓		

Digital Trust & Safety Partnership

Guiding Principle 3: Ensure assurance approaches are broadly inclusive and accessible to all users, regardless of age, socioeconomic status, race, or other characteristics.

Age Assurance Principles and Practices	DTSP Best Practices Framework				
Best Practices	Product Development	Product Governance	Product Enforcement	Product Improvement	Product Transparency
To the extent feasible and aligned with legal requirements, select age verification vendors that provide options beyond government issued IDs, such as birth certificates and school IDs, or a combined unique account identifier and picture of the user, to ensure users without access to government issued IDs are not discriminated against.		✓	✓		
Provide an accessible, easy-to-navigate appeals mechanism for those users who failed an age estimation test.			✓		
Perform an impact analysis before deploying age estimation techniques to specific populations of users to understand any discriminatory outcomes and mitigate them.	✓				
Provide a process for users to flag that a user is under age, and in concert with an enforcement action give that user in question access to an appeals process to prove their age.			✓		
Conduct reviews of age assurance implementations, including with credentialed third-party vendors or service providers as appropriate.				✓	
Consult with third parties to evaluate the impacts of age assurance methods under consideration.	✓	✓			

Digital Trust & Safety Partnership

Guiding Principle 4: Conduct layered enforcement operations to implement age assurance approaches.

Age Assurance Principles and Practices	DTSP Best Practices Framework				
Best Practices	Product Development	Product Governance	Product Enforcement	Product Improvement	Product Transparency
Set default limits on access to and discovery of the service, certain features, or particular content, subject to in-product notifications about age appropriateness of that content and/or some other form of age assurance.			✓	✓	
Label and, where appropriate, classify services as appropriate for only certain ages, and coordinate with distribution platforms to apply relevant limits for downloads and access by underage users.		✓	✓	✓	
Deploy an age assurance check if a user changes their self-declared age from one that was <18 to an age >18.			✓	✓	
Analyze behavior on a service for all users who self-declare an appropriate age at account creation, identifying users who may have inputted false information and are underage, and proactively putting these users through an additional age assurance test. Behavior indicative of a self-declaration being inaccurate might be, for example, a message celebrating a user's own 11th birthday or repeated engagement with predominantly youth-directed content.			✓	✓	
Train enforcement teams to identify indicia of a user who has mis-reported their age (for instance, their appearance signals they are actually younger), and a method for triggering further age assurance.			✓	✓	
Allow users to report users who may have mis-reported their age and thus should be limited from the service or certain features.			✓	✓	

Digital Trust & Safety Partnership

Age Assurance Principles and Practices	DTSP Best Practices Framework				
Best Practices	Product Development	Product Governance	Product Enforcement	Product Improvement	Product Transparency
Implement technical methods that can help prevent users who have failed an age assurance test and been deemed ineligible from circumventing the controls (e.g., by immediately signing up with a different account).			✓	✓	
Apply new age assurance tests to existing users as a company improves or changes its assurance processes or makes relevant changes to a product or feature.			✓	✓	
Offer family accounts in connection with parental verification by attaching a child's account to the parent's.		✓	✓	✓	
Empower users or community moderators to set age-requirements for engagement with particular content or communities within a service.		✓	✓	✓	

Digital Trust & Safety Partnership

Guiding Principle 5: Ensure that relevant age assurance policies and practices are transparent to the public, and report periodically to the public and other stakeholders regarding actions taken.

Age Assurance Principles and Practices	DTSP Best Practices Framework				
Best Practices	Product Development	Product Governance	Product Enforcement	Product Improvement	Product Transparency
Explanations why age or birth date is collected as part of account sign-up.					✓
Implementation of open source age assurance solutions, such that the implementing code can be easily inspected by external stakeholders and experts.	✓	✓			✓
Providing third party researchers access to implementation details and data on age assurance effectiveness such that evaluations of a given method's appropriateness can be made by external actors.					✓
Publishing data that explains the cost burden of different age assurance methods for providers of varying scale.					✓
Help center articles explaining a service provider's partnership with an age assurance vendor, including what data is shared and an overview of the vendor's data practices.		✓			✓
Providing quantitative and qualitative information about enforcement of age assurance policies and practices.					✓

Appendix A:
Mary Catherine Wirth Resume and Experience

Mary Catherine Wirth

Experienced legal executive who has developed and led global law enforcement response, litigation, Trust & Safety, anti-CSAM, and children's privacy / safety programs for some of the largest technology companies in the world.

Education / Bar Membership / Certifications:

- **J.D. 1992** – **University of California, Hastings College of the Law**
- **B.A. History 1989 – University of California, Davis**
- **Certified Information Privacy Professional (CIPP/US)**
- **CA State Bar # 163791**

Relevant Work Experience:

Principal, Content Law Strategies: (2019 to present)

Provide knowledgeable, practical child safety, privacy, CSAM detection & prevention, content moderation strategy and Trust & Safety infrastructure development guidance to technology and media companies, the venture capital firms that fund them and the law firms who advise them. Expert witness on CSAM, child safety and age assurance issues in the following litigation:

- *State of New Mexico v. Meta Platforms, Inc.*, State of New Mexico, First Judicial District Court, Santa Fe County, No. D-101-CV-2023-02838.
- *In re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation,* U.S. District Court for the Northern District of California (MDL No. 3047).

Associate General Counsel / Head of Trust & Safety - Adobe Inc. (August 2008 – July 2019)

Hired by Adobe's General Counsel to advise the company's executive leadership on global legal, compliance and infrastructure development issues related to company's transformation from traditional software provider to global cloud services company. Responsible for creating and overseeing all Adobe law enforcement response, PhotoDNA, child safety and Trust & Safety programs and supervised a blended team of lawyers, program managers, content moderators and dedicated engineering staff. Led all company negotiations with intelligence and law enforcement agencies in the U.S. and overseas. Managed Adobe relationships with anti-CSAM organizations and at related events globally, including the Technology Coalition, WePROTECT, NCMEC, Thorn & others. Regular speaker at the annual Dallas Crimes Against Children Conference / Technology Track. Mentor via the Technology Coalition to larger and smaller companies hoping to launch proactive CSAM detection programs. Also oversaw development of Adobe's GDPR compliance infrastructure, managed all children's privacy and education privacy issues, and helped manage the company's response to a 2013 data breach and related regulatory investigations and litigation.

Senior Director, International Legal – Yahoo! Inc. (August 2000 – November 2006)

Managed all of Yahoo's litigation, law enforcement response, product legal, privacy and children's safety work outside of the United States. Oversaw many of the internet's first cross-border 'free speech on the internet' civil and criminal cases in France, India, China, etc. and served as company spokesperson in high profile litigation, freedom of expression and civil liberties matters. Developed company's international law enforcement response policies and processes in the wake of 9/11 and led all negotiations with international intelligence and law enforcement agencies. Assisted with Yahoo!'s earliest efforts to eradicate CSAM from its network in the wake of landmark USDOJ "Operation Candyman" investigation, including partnerships with Google, Microsoft, NCMEC and leading imaging researchers.

Adjunct Law Professor – U.C. Hastings College of the Law (January 2001- December 2006)

Taught a comparative cyberlaw seminar for third year law students. Also taught trial advocacy.

Of Counsel – McCutchen, Doyle, Brown & Enersen (August 1997- August 2000)

Litigated cases in state and federal court, including a six week jury trial in *Stapper vs. GMI Holdings, Inc.* (successful verdict in favor of defendant, Genie, in product liability lawsuit brought by severely injured San Francisco firefighter), represented Japan's largest architectural firm in construction liability mediations related to a billion-dollar semi-conductor fab disaster in Taiwan, represented Stanford University in construction litigation and real estate matters, and represented the San Francisco Examiner and other media clients in defamation and anti-SLAPP matters. Handled pro bono litigation on behalf of California prisoners in partnership with the Prison Law Office. Also handled pro bono class action litigation on behalf of California trade school students who had been scammed into taking on massive student load debt.

Media Litigation Counsel – Fox Inc. (February 1996 - February 1997)

Oversaw media law / defamation / First Amendment litigation and disputes for all Fox media and entertainment companies in the U.S., including Fox Television, News Corporation and Twentieth Century Fox Film Corporation.

Litigation Counsel – O'Melveny & Myers LLP (October 1992 – January 1996)

Represented Fox Inc. and subsidiaries in media defense matters, including litigation filed against its television shows and made-for-T.V. films by O.J. Simpson and the Menendez Brothers. Provided day-to-day media law guidance to television shows like "A Current Affair." Took depositions and argued motions to dismiss and summary judgment motions in large-scale train derailment / pipeline class action. Also helped coach John Marshall High School mock trial team and handled pro bono cases for AIDS patients in partnership with AIDS Project Los Angeles.

Sample Volunteer/Personal:

- Owner – Firehorse Farm, Bainbridge Island, WA (2021-present): own and manage a small farm dedicated to animal rescue and rehabilitation (primarily, horses, ponies, goats and dogs).
- Advisor – Luminate Foundation (2019-2020): advisor to Pierre Omidyar's Luminate Foundation, helping develop responsible child safety best practices for VC investor community.
- Board Member – Willow Creek Academy, Sausalito CA (2011-2015): board member of public, Title I charter school in Sausalito, CA.

Appendix B:
Materials Considered

APPENDIX B: MATERIALS CONSIDERED

Depositions and Related Materials

1. Deposition of Ravi Sinha, December 5-6, 2024, and exhibits included therein.
2. Deposition of Guy Rosen, February 19-20, 2025, and exhibits included therein.
3. Deposition of Antigone Davis, March 4-5, 2025, and exhibits included therein.
4. Deposition of Nick Clegg, March 20-21, 2025, and exhibits included therein.
5. Deposition of Allison Hartnett, June 16-17, 2025, and exhibits included therein.

Expert Reports

1. McDaniel Expert Report (November 21, 2025 Trial Report and December 15, 2025 Corrected Trial Report)

Pleadings, Discovery Responses, and Other Court Filings

1. Meta's Responses and Objections to Plaintiffs' First Set of Interrogatories, dated June 28, 2024.
2. Order Largely Denying in Part Meta's Motion to Dismiss the Multistate Attorneys General Complaint, dated October 15, 2024.
3. Meta's Responses and Objections to Plaintiffs' Second Set of Interrogatories, dated November 22, 2024.
4. Meta's Third Supplemental and Amended Responses and Objections to Plaintiffs' Second Set of Interrogatories, dated February 28, 2025.
5. Meta's First Supplemental Responses and Objections to Plaintiffs' Fifth Set of Interrogatories, dated March 17, 2025.
6. State Attorneys' General's Affirmative Letter Brief Explaining Grounds for Anticipated Motions for Summary Judgment and *Daubert* Motions, dated November 19, 2025.
7. State Attorneys' General's Affirmative Letter Brief Explaining Grounds for Anticipated Motions for Summary Judgment and *Daubert* Motions, dated December 3, 2025.

Produced Documents

1. META3047MDL-012-00000001
2. META3047MDL-012-00000096
3. META3047MDL-014-00368074
4. META3047MDL-014-00371983
5. META3047MDL-019-00129336
6. META3047MDL-022-00008803
7. META3047MDL-033-00103930
8. META3047MDL-034-00007909
9. META3047MDL-034-00081054
10. META3047MDL-034-00098929
11. META3047MDL-034-00152714
12. META3047MDL-037-00088546
13. META3047MDL-037-00088547
14. META3047MDL-037-00118789
15. META3047MDL-040-00000321
16. META3047MDL-040-00000322
17. META3047MDL-040-00000323
18. META3047MDL-040-00000327

19. META3047MDL-040-00000333
20. META3047MDL-040-00000350
21. META3047MDL-040-00000354
22. META3047MDL-040-00000356
23. META3047MDL-040-00000365
24. META3047MDL-040-00335514
25. META3047MDL-047-00016158
26. META3047MDL-047-00461683
27. META3047MDL-047-01163613
28. META3047MDL-053-00012657
29. META3047MDL-053-00012709
30. META3047MDL-065-00004636
31. META3047MDL-065-00017555
32. META3047MDL-072-00039030
33. META3047MDL-091-00080707
34. META3047MDL-129-00092478
35. META3047MDL-146-00072800
36. META3047MDL-146-00072824
37. META3047MDL-190-00000001
38. META3047MDL-203-00218141
39. META3047MDL-203-00315720
40. META3047MDL-208-00003249
41. META3047MDL-208-00003306
42. META3047MDL-208-00003307
43. META3047MDL-208-00003308
44. META3047MDL-208-00003310
45. META3047MDL-208-00050921
46. META3047MDL-208-00051182
47. META3047MDL-208-00061837
48. META3047MDL-208-00061837
49. META3047MDL-208-00061873
50. META3047MDL-217-00000218
51. META3047MDL-040-00000343
52. META3047MDL-046-00068729
53. META3047MDL-012-00000056
54. META3047MDL-146-00072880
55. META3047MDL-003-00047875
56. META3047MDL-208-00003312
57. META3047MDL-143-00000358

Public Sources

1. FTC Business Guidance https://www.ftc.gov/business-guidance

2. DTSP "Age Assurance Guiding Principles and Best Practices" (September 2023) https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

3. Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946–2966 (Dec. 17, 2002).

4. Federal Information Security Modernization Act, 44 U.S.C. §§ 3551–3558.

5. Wikipedia, Federal Information Security Management Act of 2002 at https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

6. Adobe Common Controls Framework at https://www.adobe.com/trust/compliance/adobe-ccf.html

7. Children's Online Privacy Protection Rule, Federal Register / Vol. 90, No. 76 / Tuesday, April 22, 2025 / Rules and Regulations

8. Institute of Electrical and Electronics Engineers (IEEE) https://www.ieee.org/

9. IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children at https://5rightsfoundation.com/wp-content/uploads/2024/09/2089-2021-with-disclaimer.pdf.

10. IAPP "Children's Privacy Laws and Freedom of Expression: Lessons from the UK Age-Appropriate Design Code" (Nov 13, 2023) at https://iapp.org/news/a/childrens-privacy-laws-and-freedom-of-expression-lessons-from-the-uk-age-appropriate-design-code

11. Children's Online Privacy Protection Rile, 90 Fed. Reg. 16961 (Apr. 22, 2025)

12. *Free Speech Coalition, Inc. v. Paxton,* No 23-1122, 606 U.S. _ (2025)

13. Leading Technology Companies Launch Initiative to Promote a Safer and More Trustworthy Internet – Digital Trust & Safety Partnership (February 18, 2021 press release announcing the launch of the Digital Trust & Safety Partnership, "a first-of-its-kind initiative aimed at promoting a safer and more trustworthy internet.") at https://dtspartnership.org/press-releases/leading-technology-companies-launch-initiative-to-promote-a-safer-and-more-trustworthy-internet/

14. About NIST, https://www.nist.gov/about-nist.

15. *About Instagram Teen Accounts*, Instagram Help Center at https://help.instagram.com/995996839195964/

16. *Best Practice*, Computer Security Resource Center, https://csrc.nist.gov/glossary/term/best_practice.

17. *Best Practice*, Merriam Webster, https://www.merriam-webster.com/dictionary/best%20practice.

18. *Bringing local context to our global standards*, Meta Transparency Center (Jan. 18, 2023) at https://transparency.meta.com/policies/improving/bringing-local-context/.

19. *Community Standards Enforcement Report*, Meta Transparency Center, https://transparency.meta.com/reports/community-standards-enforcement/.

20. *Complying with COPPA: Frequently Asked Questions (FTC COPPA FAQ)*, FTC, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.
21. *COPPA Rule*, FTC, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protectionrule-coppa
22. *Counting Strikes*, Meta Transparency Center, https://transparency.meta.com/enforcement/taking-action/counting-strikes/ (elaborating on consequences for violations).
23. Dan Milmo & Josh Taylor, *Meta to put under-18 Instagram users into new 'teen accounts*,' The Guardian (Sep. 14, 2024), https://www.theguardian.com/technology/2024/sep/17/meta-instagram-facebook-teen-accounts-social-media-ban-australia?utm_source=chatgpt.com.
24. *Helping reviewers make the right calls*, Meta (Nov. 12, 2024) at https://transparency.meta.com/enforcement/detecting-violations/making-the-right-calls/.
25. *History of Facebook*, Wikipedia, https://en.wikipedia.org/wiki/History_of_Facebook.
26. *How enforcement technology works*, Meta Transparency Center (Nov. 12, 2024) at https://transparency.meta.com/enforcement/detecting-violations/how-enforcement-technology-works/.
27. *How Meta invests in technology*, Meta Transparency Center (Jan. 19, 2022) at https://transparency.meta.com/enforcement/detecting-violations/investing-in-technology/.
28. *How Meta trains technology*, Meta Transparency Center (Jan. 19, 2022) at https://transparency.meta.com/enforcement/detecting-violations/training-technology/.
29. *How review teams work*, Meta Transparency Center (Nov. 12, 2024) at https://transparency.meta.com/enforcement/detecting-violations/how-review-teams-work/.

30. *How teams are trained*, Meta Transparency Center (Nov. 12, 2024) at https://transparency.meta.com/enforcement/detecting-violations/training-review-teams/.
31. *How technology detects violations*, Meta Transparency Center (Oct. 18, 2023) at https://transparency.meta.com/enforcement/detecting-violations/technology-detects-violations/.
32. *How technology helps prioritize review*, Meta (Jan. 19, 2022) at https://transparency.meta.com/enforcement/detecting-violations/technology-helps-prioritize-review/.
33. *How we assess and prepare for global risk*, Meta Transparency Center (Apr. 29, 2024) at https://transparency.meta.com/enforcement/detecting-violations/how-we-assess-global-risks/.
34. *Introducing New Ways to Verify Age on Instagram*, Meta, https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/.
35. *Introducing Stricter Message Setting for Teens on Instagram and Facebook*, Meta Newsroom (Jan. 25, 2024) at https://about.fb.com/news/2024/01/introducing-stricter-message-settings-for-teens-on-instagram-and-facebook/.
36. *Timeline of tools, features, and resources to help support teens and parents* *https://www.meta.com/help/policies/809291991003600/?srsltid=AfmBOoovWKiEQyytdRQgNHa9I9UB1e7E59-ONYMceVgj7KZJPSe1JqUt*
37. Julie Jargon, *Instagram Is Restricting Teen Accounts-and Blocking Sneaky Workarounds*, The Wall Street Journal (Sep. 17, 2024), https://www.wsj.com/tech/personal-tech/instagram-is-restricting-teen-accountsand-blocking-sneaky-workarounds-893ff8d0?utm_source=chatgpt.com.
38. Letter from Meta to Richard Durbin (Apr. 19, 2024), https://www.judiciary.senate.gov/imo/media/doc/2024-01-31_-_qfr_responses_-_zuckerberg1.pdf.
39. *One Set of Community Standards*, Meta Transparency Center (Nov. 11, 2024), https://transparency.meta.com/community-standards-unified.
40. *Our tools, features and resources to help support teens and parents*, Meta Help Center.

41. *Safety Center*, Meta Safety Center, https://about.meta.com/actions/safety/.
42. *Teen Privacy and Safety Settings*, Meta Help Center, https://www.meta.com/help/policies/1754656424993737/?srsltid=AfmBOor0vKrKXjLn1MDu4le8dMhpSwcMPLpJe-lT17brs6eH3DNhB0b.
43. *The community standards apply the same to everyone, everywhere*, Meta Transparency Center (Nov. 12, 2024) at https://transparency.meta.com/policies/improving/policies-apply-to-everyone-everywhere/.
44. *The people behind Meta's review teams*, Meta Transparency Center (Jan. 19, 2022) at https://transparency.meta.com/enforcement/detecting-violations/people-behind-our-review-teams/.
45. EY, Independent Audit on Facebook For the Period of 29 August 2023 to 30 June 2024 (Aug. 2024), https://transparency.meta.com/reports/regulatory-transparency-reports/.
46. EY, Independent Audit on Instagram For the Period of 29 August 2023 to 30 June 2024 (Aug. 2024), https://transparency.meta.com/reports/regulatory-transparency-reports/.
47. Ben Bradford, et al., *Report of The Facebook Data Transparency Advisory Group*, Yale Law School: The Justice Collaboratory (Apr. 2019).
48. **Account registration pages and workflows:**
    a. X/Twitter: https://x.com/signup
    b. Google: https://accounts.google.com/signup
    c. Apple: https://account.apple.com/
    d. Adobe: https://account.adobe.com/
    e. Microsoft: https://signup.live.com
    f. Snap: https://accounts.snapchat.com/v2/signup?locale=en-US
    g. TikTok: Application available to download via https://apps.apple.com/us/app/tiktok-videos-shop-live/id835599320
    h. Facebook: https://www.facebook.com/r.php?entry_point=login
    i. Instagram: https://www.instagram.com/sem/campaign/emailsignup
49. *Are new global age verification requirements creating a children's online safety legal patchwork?,* Int'l Ass'n Priv. Pros. ("IAPP") (August 14, 2025) at https://iapp.org/news/a/are-new-global-age-verification-requirements-creating-a-children-s-online-safety-legal-patchwork-.

50. *CIPP/US: Certified Information Privacy Professional/United States*, IAPP, at https://iapp.org/certify/cippus/

51. *About Us*, Digital Trust & Safety Partnership ("DTSP") (listing DTSP's "partners"), https://dtspartnership.org/#aboutus.