Knight Georgetown Institute

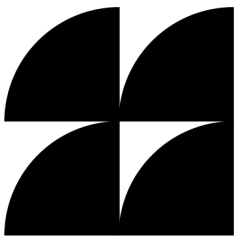
TECH JUSTICE LAW

USC Marshall School of Business
Neely Center for Ethical Leadership and Decision Making

MAY 2026

Designing Technology Remedies

Lessons for Social Media and Generative AI Chatbot Litigation



Authors

Peter Chapman
Knight-Georgetown Institute

Alissa Cooper
Knight-Georgetown Institute

Amy Winecoff
Knight-Georgetown Institute

Tiffany Gillis Brown
Tech Justice Law

Melodi Dinçer
Tech Justice Law

Meetali Jain
Tech Justice Law

Sarah Kay Wiley
Tech Justice Law

Ravi Iyer
USC Marshall Neely Center

About the Knight-Georgetown Institute

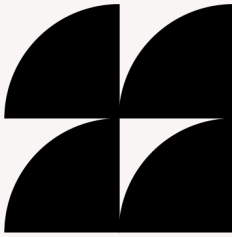
The Knight-Georgetown Institute (KGI) is dedicated to connecting independent research with technology policy and design. KGI serves as a central hub for the growing network of scholarship that seeks to shape how technology is used to produce, disseminate, and access information. KGI is designed to provide practical resources that policymakers, journalists, and private and public sector leaders can use to tackle information and technology issues in real time. Georgetown University and the Knight Foundation came together to launch the institute in 2024. Learn more about KGI at https://kgi.georgetown.edu.

About Tech Justice Law

Tech Justice Law (TJL) is dedicated to advancing accountability, transparency, and justice in the technology sector. TJL uses strategic litigation, policy advocacy, and public education to challenge abuses of power by technology corporations and defend the rights of individuals and communities harmed by emerging technologies. TJL partners with regulators, grassroots organizations, advocates, and scholars to challenge technologies that contribute to harm, fight discriminatory practices, and build a future where technology serves the public good rather than undermines it. TJL has served as co-counsel representing multiple individuals in cases before state and federal courts challenging the harms associated with chatbot technologies, and has authored or facilitated over two dozen amicus briefs in leading tech accountability cases.

About the USC Marshall Neely Center

The USC Marshall's Neely Center for Ethical Leadership and Decision Making has unique expertise at the connection between academia, civil society, government, and technology companies. The Neely Center's Design Code for Social Media has influenced legislation and litigation across US states, in the UK, EU, and has been used by civil society groups in places as diverse as Kenya and Indonesia. More broadly, the Neely Center maintains a leadership position in technology design space and is regularly consulted by companies, policymakers, litigators, and civil society groups, including collaborations with Ofcom, Google Jigsaw, the Anxious Generation team, and numerous civil society organizations.



Acknowledgments

The authors thank Taylor Courtney, Iverson Yue, and Rachel Kim of Georgetown University, Julia Jellema-Butler of Yale University, and Taylor Gray of Emory University for their valuable research assistance in the development of this framework. The authors also extend their gratitude to participants of the November 2025 Litigating Platform Design convening at Georgetown University for their insights.

The authors further wish to recognize the contributions of the KGI team, including Julie Anne Miranda-Brobeck, Zander Arnao, and Minhua Li, as well as the TJL team, including Maddy Batt.

Executive Summary

Social media and generative AI chatbot companies are facing an expanding wave of litigation involving hundreds of plaintiffs and dozens of cases in federal and state courts across the United States. Historically, many claims against social media companies were dismissed under Section 230 of the Communications Decency Act and the First Amendment. This pattern has shifted. Courts are increasingly allowing claims against social media and AI chatbot companies to proceed to discovery and trial. As a result, courts are emerging as central actors in shaping technology policy.

Court decisions – particularly at the remedy phase – will impact the design, governance, and accountability of social media and AI chatbot platforms. Remedies may impose monetary damages or require a company to change their behavior. Monetary damages alone are unlikely to meaningfully improve safety. Lessons from technology, tobacco, pharmaceuticals, and e-cigarette litigation suggest that durable change in company conduct typically requires a combination of monetary damages and court-ordered changes to company behavior to protect consumers. Crafting effective remedies for social media and AI chatbot companies requires careful consideration of complex issues related to product design, transparency, accountability, and ongoing oversight.

Designing Technology Remedies offers a practical, evidence-based framework for addressing these issues. Developed by the Knight-Georgetown Institute (KGI), Tech Justice Law (TJL), and the USC Marshall's Neely Center for Ethical Leadership and Decision Making (USC Neely Center), the framework was developed through a systematic review of nearly 100 prior remedies, including Federal Trade Commission (FTC) consent decrees, public health litigation, civil rights settlements, and technology-related cases. These findings were assessed through stakeholder interviews and multidisciplinary convening involving the offices of state attorneys general, plaintiffs' attorneys, technologists, researchers, and legal scholars. *Designing Technology Remedies* is intended to help litigators, courts, and policymakers identify and implement effective and enforceable remedies that are responsive to specific social media and AI chatbot harms.

The framework organizes recommended remedies into three complementary categories:

- **Harm Prevention** remedies change how companies design, develop, and deploy their products. Recommended remedies include prohibitions on unsafe design features; safer default settings for minors and other users; meaningful limits on data collection, retention, and use; restrictions on targeted advertising to minors; data deletion and disgorgement where data was unlawfully obtained; and age assurance safeguards in appropriate circumstances.
- **Harm Mitigation** remedies give users tools to report, avoid, and respond to harmful experiences. Recommended remedies include accessible and effective user and parental controls, measured against outcome-based metrics; effective account and data deletion; data portability; and user-reporting systems with concrete response timelines, escalation processes, and communication to the reporting user.

- **Governance** remedies change how companies make decisions, exercise leadership oversight, enable independent scrutiny, and enforce compliance. Recommended remedies include a senior compliance officer with cross-functional authority; alignment of organizational goals with remedy objectives; an independent external monitor with audit authority; internal and external measurement, including universal-holdout experiments and independently administered user surveys; and transparency mechanisms, including publicly accessible document repositories and safe-harbor for independent research.

Effective remedies will combine all three categories. Prevention, mitigation, and governance are mutually reinforcing; no single category is sufficient on its own for addressing harm.

The *Designing Technology Remedies* framework is intentionally flexible rather than prescriptive. Not every remedy will apply in every case. The appropriate approach will depend on the specific harms, the nature of the defendant's product, and the procedural posture of the litigation. At the same time, the framework identifies several commonly used remedies that may underperform, including standalone employee training requirements or consent-based remedies for targeted data use or data sharing.

The growing body of social media and AI chatbot cases now moving through federal and state courts presents a critical opportunity to translate available research and evidence into durable and enforceable change. Well-designed remedies – paired with effective oversight and enforcement – are essential for improving safety online. *Designing Technology Remedies* is intended to support this effort.

Table of Contents

I. Introduction

United States courts have become a focal point for those seeking accountability from social media and generative AI chatbot companies. Private plaintiffs, school districts, and attorneys general from states across the country have filed hundreds of cases on behalf of consumers, minors, families, and states. Their claims focus on harms arising from the design of social media platforms and AI chatbots, including addiction and compulsive use, unwanted contact, and privacy violations.[1] Complaints are based on a range of legal theories, including negligence, failure to warn, consumer protection, deceptive trade practices, and public nuisance.[2]

Historically, social media platforms have successfully moved to dismiss cases under Section 230 of the Communications Decency Act and the First Amendment. This pattern has shifted. Lawsuits against social media and AI chatbot companies are increasingly surviving these defenses at the motion to dismiss stage and entering previously uncharted territory, such as discovery in which plaintiffs are empowered to seek relevant documents and information from defendants.

By mid 2026, several social media cases had moved to trial and remedy. As of this writing, a New Mexico jury has ordered Meta to pay $375 million for misleading consumers and endangering children.[3] A California jury found Meta and Google substantially responsible for harms flowing from a plaintiff's social media addiction, awarding $6 million.[4] Snap and TikTok settled similar claims before trial.[5] Claims against Meta, Snap, TikTok, and YouTube are consolidated in a multidistrict litigation in federal court.[6]

Following the public launch of ChatGPT in late 2022, plaintiffs have filed multiple cases related to harms alleged to arise from the use of AI chatbots. Private plaintiffs have brought cases against Character.AI,[7] OpenAI,[8] and Google.[9] A broad, bipartisan coalition of attorneys general is also focused on chatbot risks, warning AI developers that "you will be held accountable for your decisions."[10] Several attorneys general have opened investigations or filed cases against AI chatbot companies.[11] The plaintiff in the first case against an AI chatbot company prevailed at the motion to dismiss stage,[12] with Character.AI and Google ultimately settling claims before the case went to trial.[13]

---

[1] Knight-Georgetown Institute et al., "Taxonomy."
[2] Tech Justice Law, "Tech Related Actions and Litigation."
[3] New Mexico Department of Justice, "New Mexico Department of Justice Wins Landmark Verdict Against Meta."
[4] Allyn, "Jury finds Meta and Google negligent in social media harms trial."
[5] Kang, "Snap Settles Social Media Addiction Lawsuit Ahead of Landmark Trial"; Kang, "TikTok Settles Social Media Addiction Lawsuit Ahead of a Landmark Trial."
[6] United States Judicial Panel on Multidistrict Litigation, "Pending MDL Dockets by District."
[7] Tech Justice Law, "Big Win in our Character AI Lawsuit!"
[8] Social Media Victims Law Center and Tech Justice Law, "Lawsuits accuse ChatGPT of emotional manipulation."
[9] Bellan, "Father Sues Google, claiming Gemini chatbot drove son into fatal delusion."
[10] National Association of Attorneys General, "Joint Letter to AI Industry Leaders on Child Safety."
[11] Grout, "AG Coleman Sues AI Chatbot Company for Preying on Children"; Helmore, "Florida to open criminal investigation into OpenAI over ChatGPT's influence on alleged mass shooter."
[12] Order, Garcia v. Character Techs., Inc., No. 6:24-cv-1903-ACC (M.D. Fla. May 21, 2025).
[13] Rocha, "Google and Character.AI to Settle Lawsuit Over Teenager's Death."

Harmful product design decisions at issue in cases against social media and AI chatbot companies can occur when the incentives of companies are not fully aligned with the safety and wellbeing of users or the public. For example, to encourage higher levels of user engagement, companies might use deceptive design practices that extend product use. This in turn can harm consumers by negatively affecting their sleep quality,[14] emotional well-being,[15] ability to maintain meaningful real-world relationships,[16] or professional performance.[17]

Historically, litigation has played an important role in shaping regulation of tobacco, pharmaceuticals, gambling products, consumer product safety, and other sectors.[18] The cases against social media and AI chatbot companies advancing through different courts may prove to be just as critical in creating accountability, requiring product design changes and safeguarding the public from harm.

Each of those outcomes are contingent on the end result of these cases: namely what remedies are ordered by courts or negotiated through settlement. When considering injunctive relief (obligations affecting a company's conduct), the stakeholders involved in cases against social media and AI chatbot companies are faced with numerous novel questions about how to craft remedies that effectively prevent the harms that spurred the litigation originally. How should remedies influence a company's design and data practices? What types and levels of transparency into potentially proprietary company practices should remedies provide, to whom, and for what specific purposes? And how can attorneys general and private plaintiffs most effectively monitor and, where necessary, enforce compliance?

Designing Technology Remedies is a framework developed by KGI, TJL, and the USC Neely Center to inform litigators, courts, and policymakers designing effective remedies in litigation involving social media and AI chatbot companies. Drawing on expert input and systematic analysis of remedies across other sectors, the framework identifies practical, evidence-based approaches to injunctive relief aimed at preventing and addressing harms linked to technology product design and data practices.

The framework organizes potential remedies into three core categories:

- Harm Prevention
- Harm Mitigation
- Governance

The framework is intended to inform ongoing and future cases during the remedy and settlement phases, where decisions about product design, transparency, accountability, and oversight have the potential to profoundly affect the broader technology ecosystem. While this framework is focused on the US context, these cases are being watched by litigators and regulators around the world for precedents as to what remedies are possible in other contexts.

---

[14] Ndubisi et al., "Social Media Use and Sleep Quality in Adolescents and Young Adults."
[15] Faviero et al., "Teens, Social Media, and Mental Health."
[16] Phang et al., "Investigating Affective Use and Emotional Well-being on ChatGPT."
[17] Zivnuska et al., "Social media addiction and social media reactions"; Smutny and Sudzina, "What Affects Work Performance When Using AI Chatbots?"; Kosmyna et al., "Your Brain on ChatGPT."
[18] Engstrom and Rabin, "Pursuing Public Health Through Litigation."

Since 2024, KGI, TJL, and the USC Neely Center have convened state attorneys general offices, private litigators, technology researchers, and legal scholars to identify priorities, document lessons learned, and develop practical resources. *Designing Technology Remedies* reflects the wealth of insights shared by these experts, as well as our analysis of nearly 100 remedies across sectors, including FTC consent decrees, public health litigation, civil rights settlements, and technology litigation. We systematically analyzed these cases to identify effective practices and opportunities for strong and impactful remedies in social media and AI chatbot litigation.

The framework is organized as follows: Section II provides an overview of the remedy framework. Sections III, IV, and V explain each category of remedies – harm prevention, harm mitigation, and governance, respectively. Section VI concludes. Details about our methodology are included in the Appendix.

II. Remedy Framework Overview

Social media and AI chatbot litigation raises claims concerning harms that trace back to company product design choices, which in turn reflect the industry's broader business and financial motivations. Experience litigating harms in complex cases, including within tobacco, pharmaceutical, and e-cigarette industries, suggests that monetary damages alone were unable to dislodge entrenched business practices and conduct. Social media and AI chatbot remedies should involve a combination of monetary and injunctive relief to effectively respond to harms and help prevent future harms from occurring.

Monetary relief requires one party to compensate one or more parties for direct losses, indirect consequences, and other costs incurred as a result of the alleged wrongdoing.[19] Injunctive relief, on the other hand, compels a party to either perform a specific action or to cease a particular action to address wrongdoing.[20]

Monetary relief will likely be a core element of remedies related to social media and AI chatbot litigation.[21] Monetary relief could require damages, costs, attorneys' fees, or other specific payments, including allocations to support public interest programming or independent research.[22] Monetary relief alone, however, is unlikely to prevent future harm, especially where companies can easily absorb such payments through ongoing profits and valuations. For these reasons, complaints against social media and AI chatbot companies have included demands for design change, transparency, oversight, as well as other injunctive remedies.

---

[19] Legal Information Institute, "monetary relief."
[20] Legal Information Institute, "settlement."
[21] New Mexico Department of Justice, "New Mexico Department of Justice Wins Landmark Verdict Against Meta."
[22] *See*, *e.g.*, Order Granting Final Settlement Approval, *In re* Google Location History Litigation, No. 5:18-cv-05062-EJD (N.D. Cal. May 3, 2024); Master Settlement Agreement, Mississippi v. Philip Morris Inc., No. 94-1429 (Nov. 23, 1998) [hereinafter MSA]. In Google, the settlement order proposes *cy pres* awards and recipients. The MSA requires monetary support for public education initiatives, youth smoking prevention programs, grants to states for tobacco education, and research on tobacco-related diseases.

The *Designing Technology Remedies* framework focuses on potential injunctive relief that may prevent and mitigate harm from social media and AI chatbot product design. The framework is organized around three overarching themes: harm prevention, harm mitigation, and governance. The framework includes a full set of possible remedies, based on previous precedent as well as understandings of technology's role in harm. However, in any given case, the case circumstances will inform which specific remedies are possible and effective. Not all remedies will apply in all cases. The *Designing Technology Remedies* framework is intended to be actionable for litigators in specific cases as well as policymakers more broadly.

The following table summarizes recommended remedies across harm prevention, harm mitigation, and governance. Analysis of each remedy includes examples from outside of the technology industry so as to learn from cases where remedies sought to address complex and systemic harms. These examples can inform remedies related to specific social media and AI chatbot cases.

A. Overview of Technology Remedies

Category	Requirement	Remedy Description
HARM PREVENTION REMEDIES Harm prevention remedies seek to prevent the occurrence of future harm by requiring companies to change how they design, develop, and deploy their products and features.		
Product Design	Prohibition of Unsafe Designs	Remedies should prohibit the use of specific unsafe design features that cause or contribute to the harms alleged in litigation.
	Safer Default Settings	Where prohibition of unsafe designs for all users is not appropriate, remedies should require companies to default users into settings that avoid unsafe design features that cause or contribute to the harms alleged in litigation.
Data Collection and Minimization	Limits on Data Collection, Retention, and Use	Remedies should establish limits on data collection, retention, and use, and, where appropriate, include requirements for data destruction.
	Restrictions on Data Access and Transfers	Remedies should establish permissible uses of data and require internal data access controls limited to approved use cases.
	Restrictions on Targeted Advertising	Remedies should prohibit the collection and use of minors' personal data for targeted advertising.
	Data Deletion and Disgorgement	When companies collect data unlawfully, remedies should specifically require data deletion or disgorgement of wrongful benefits.
Age Assurance	Age Assurance Safeguards	Where remedies require the company to provide specific protections to users based on their age, they should also require that the age assurance mechanisms the company adopts follow best practices for preserving privacy, accessibility, and efficacy.

HARM MITIGATION REMEDIES Harm mitigation remedies are measures that give users tools to report, avoid, or respond to harmful experiences on digital platforms.		
Product Controls	User Controls	Remedies should require platforms to provide accessible and effective user safety, privacy, and time management tools.
	Parental Controls	Remedies should require platforms to provide easily accessible and effective parental control tools for guardians of minors.
User Data Controls	Account and Data Deletion	Remedies should require platforms to provide users with accessible tools to delete or deactivate their accounts and their associated data.
	Data Portability	Remedies should require platforms to enable data portability, giving users meaningful ability to export their data.
Reporting and Removal	User Reporting and Removal	Remedies should require effective user reporting mechanisms and concrete expectations for how platforms respond.
GOVERNANCE REMEDIES Governance remedies are measures designed to influence how a company makes decisions, exercises leadership oversight, and enforces compliance specific to the remedies.		
Internal Governance Requirements	Compliance Officer	Remedies should require the company to designate a senior-level compliance officer, supported by a cross-functional committee, responsible for ensuring and embedding compliance across all elements of the remedy.
	Organizational Goals	Remedies should require the company to ensure that product, performance, and compensation goals and implementation structures align with remedy goals.
Monitoring and Measurement	Independent Monitor	Remedies should establish an independent monitor to ensure compliance through a regular reporting schedule and periodic audits by qualified independent auditors.
	Measurement Mandates	Remedies should require internal and external measurement and reporting of specific metrics responsive to the harms alleged in litigation.
	Transparency Mechanisms	Remedies should require the establishment of a document repository for documents relevant to litigation as well as guarantee researcher access to data relevant to the harms alleged in litigation.

B. Harm Prevention

Harm prevention remedies seek to prevent the occurrence of harm by requiring companies to change how they design, develop, and deploy their products and features.

A wide set of product design decisions can contribute to harmful or unwanted experiences for users. Companies can alter their product designs to better prevent harms from occurring, for example through removing or reducing engagement-based optimization or changing default account visibility. These design changes can be effective at preventing harms because they proactively modify features that are the source of specific harms. Such measures, however, rely on the proactive identification and modification of harmful design practices throughout the product lifecycle from initial ideation to pre-deployment evaluation and to post-deployment monitoring. Such harmful practices are increasingly well understood for social media, and similar practices are beginning to be identified for AI chatbots.[23]

Harm prevention remedies are discussed in detail in Section III.

C. Harm Mitigation

Harm mitigation remedies are measures that give users tools to report, avoid, or respond to harmful experiences with social media and AI chatbot companies.

Companies can provide user tools to customize their experiences. They may create systems to report and remove harmful content on their platforms or for users to try to prevent harmful or unwanted experiences. Historically, user uptake of harm mitigation tools and user controls on digital platforms has been low.[24] Mitigation is limited by the imperfect identification of harm, whether by platforms or by consumers, as well as the effectiveness of safety tools and the ability or willingness of users to understand and use provided tools. Still, it is important for users to haved recourse when they encounter unwanted or harmful experiences, even if only a minority of harmed users might effectively use such options.

Harm mitigation remedies are discussed in detail in Section IV.

[23] Knight-Georgetown Institute et al., “Taxonomy.”

[24] Expert Report of Dimitri A. Christakis, *In re* Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal. Dec. 11, 2025); Cunningham et al., “Ranking by engagement and non-engagement signals.”

D. Governance

Governance remedies are measures designed to influence how a company makes decisions, exercises leadership oversight, and enforces compliance specific to the remedies.

Injunctive relief focused on companies' internal governance processes, including decisions about product design, development, and deployment, are intended to bring companies' incentives more in line with consumer safety. The motivating idea for governance remedies is that mandates for better internal processes combined with transparency for specific external parties – including state attorneys general, users, and researchers – will reduce the frequency with which companies make harmful design decisions. Better governance can ultimately improve not only the design practices at issue in a case, but also disincentivize and, ideally, prevent harmful design practices from moving forward.

Governance remedies are discussed in detail in Section V.

E. Excluded Remedies

The *Designing Technology Remedies* framework excludes certain categories of remedies. Within harm mitigation, the framework explicitly excludes remedies that rely primarily on user consent. Placing responsibilities with users for approving or denying practices that impact their privacy or safety has been shown to lead to what scholars have termed "consent fatigue," where frequent prompts for user consent cause users to disengage from meaningful decisionmaking.[25]

Within governance remedies, the framework excludes employee training. Training has been a ubiquitous feature of FTC consent decrees, but has not been shown to structurally improve design. While this remedy may serve specific purposes in some cases, the framework does not broadly recommend the inclusion of training mandates.[26]

III. Harm Prevention Remedies

Harm prevention remedies seek to prevent the occurrence of future harm by requiring companies to change how they design, develop, and deploy their products and features.

Intervention at this level can proactively prevent harm because these remedies do not rely on users to take steps to ensure safe experiences. This section describes harm prevention remedies in three areas: **product design**, **data collection and minimization**, and **access limitations**.

Remedies across industries regularly incorporate a range of design-based remedies, and this section describes remedies that can be relevant to social media and AI chatbot companies.

[25] Schermer et al., "The crisis of consent"; Jones, *The Character of Consent*.

[26] The framework is silent about two other categories of remedies that have surfaced in social media litigation: requirements to remove end-to-end encrypted messaging and requirements to remove ephemeral private messaging. The framework authors did not have consensus to include them in the framework but may comment on them separately in other venues.

A. Product Design

Remedies should prohibit unsafe product design features and require companies to establish safer default settings. Intervening at the level of product design can directly remove features that cause or contribute to harm.

Harm Prevention Requirements
Product Design
Prohibition of Unsafe Designs: Remedies should prohibit the use of specific unsafe design features that cause or contribute to the harms alleged in litigation.
Safer Default Settings: Where prohibition of unsafe designs for all users is not appropriate, remedies should require companies to default users into settings that avoid unsafe design features that cause or contribute to the harms alleged in litigation.

1. Prohibition of Unsafe Designs

Remedies should prohibit the use of specific unsafe design features that cause or contribute to the harms alleged in litigation.

Social media and AI chatbot lawsuits have focused on harms arising from specific design practices, including deceptive patterns, extended use designs, overly permissive account visibility, and engagement-maximizing algorithmic designs.[27] Remedies could target features that encourage overuse (e.g., infinite scroll, auto-play, ephemerality, and AI chatbot responses that invite further engagement through emotional manipulation),[28] enable unwanted contact (e.g., recommending connections between minors and untrusted adults), or mimic human behavior and increase sycophancy through anthropomorphic design or unintentionally through system training decisions.[29] Changes could apply for all users or particular groups, such as minors.

Previous remedies have prohibited unsafe designs. Settlements with automakers including Honda and General Motors, for example, required concrete changes to product design.[30] Technology settlements have included prohibitions on deceptive design, with the FTC requiring companies to modify how they notify users when their geolocation is shared[31] and modify designs for how users can revoke consent

[27] Knight-Georgetown Institute et al., "Taxonomy."
[28] De Freitas et al., "Emotional Manipulation by AI Companions."
[29] See Young People's Alliance, "A Bill to Save Human Connection From Human-Like AI Companions."
[30] Consent Judgment, District of Columbia v. General Motors Co. (D.C. Super. Ct. Oct. 9, 2017); Office of the Attorney General for the District of Columbia, "Attorney General Racine Reaches $120 Million Settlement with General Motors Company Over Defective Ignition Switches"; Office of the New York State Attorney General, "Attorney General James Announces $85 Million Multistate Settlement with Honda Over Airbag Failures."
[31] Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Amazon.com, Inc., No. 2:23-cv-00811-TL (W.D. Wash. July 19, 2023).

for billing.[32] Settlements with Meta[33] and Greystar[34] required changes to algorithmic designs. Settlements have also introduced rate limits, which are restrictions on how many requests or actions a user can perform within a given period of time. A settlement with Thomson Reuters, for example, modified default settings to restrict the total number of search results returned by the platform's person search tool.[35] A settlement with JUUL established purchase volume limits that were designed to prevent bulk purchasing that purportedly enabled resale to minors.[36]

2. Safer Default Settings

Where prohibition of unsafe designs for all users is not appropriate, remedies should require companies to default users into settings that avoid unsafe design features that cause or contribute to the harms alleged in litigation.

Default settings have an outsized impact on user experience. When companies enable a setting by default, most users keep it. When they do not, users rarely activate the feature.[37] Internal company documents released in social media litigation show how default features are more widely used.[38] Remedies should require companies to change default settings where they can be used to prevent harms alleged in litigation.

Where litigation relates to minors, the remedy should require that they are defaulted into settings that prevent the harms alleged in litigation. In the context of AI chatbots, this should include mandating a default product version without human-mimicking features for minors.[39]

Where a user changes safety defaults, the user's interface should visibly inform them about risks associated with their current configuration.[40] The visual indicators should be designed, tested, and localized appropriately such that the indicators' meanings are properly conveyed to users. Where a minor's account is paired with a parental account, the company should provide regular, conspicuous reminders of the parent's ability to modify settings to safer experiences.

There is precedent for changing default experiences within existing technology remedies. A settlement with Thomson Reuters required the company to change default user settings to provide greater privacy by default.[41] A settlement with Epic Games also targeted the change of default settings,

[32] Decision and Order, Epic Games, Inc., FTC Docket No. C-4790 (Mar. 14, 2023).
[33] Austin, "An Update on Our Ads Fairness Efforts."
[34] United States Department of Justice, "Justice Department Reaches Proposed Settlement with Greystar, the Largest U.S. Landlord, to End Its Participation in Algorithmic Pricing Scheme."
[35] Class Action Settlement Agreement, Brooks v. Thomson Reuters Corp., No. 3:21-cv-01418-EMC (N.D. Cal. Aug. 29, 2024).
[36] Consent Judgment, Minnesota v. JUUL Labs, Inc., No. 27-CV-19-19888 (Minn. Dist. Ct. Hennepin Cnty. May 16, 2023).
[37] Cunningham et al., "Ranking by engagement and non-engagement signals"; Shakhina et al., "How Does the Design of Social Media Content Controls Shape Users' Choice?"
[38] TikTok, for example, disclosed adoption rates for default and non-default safety features. Expert Report of Dimitri A. Christakis, ¶ 664, *In re* Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal. Dec. 11, 2025). *See also* Plaintiffs' Corrected Omnibus Opposition to Defendants' Motions for Summary Judgment at 45, *In re* Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (PHK) (N.D. Cal. Jan. 26, 2026).
[39] See Young People's Alliance, "A Bill to Save Human Connection From Human-Like AI Companions."
[40] See Jakob Nielsen, "How I Developed the 10 Usability Heuristics."
[41] Class Action Settlement Agreement, Brooks v. Thomson Reuters Corp., No. 3:21-cv-01418-EMC (N.D. Cal. Aug. 29, 2024).

requiring that Epic change default settings for children by turning off features with voice and text user-to-user communications.[42]

B. Data Collection and Minimization

The remedy should introduce constraints on how companies collect and use personal data. Specific remedies should include limits on data collection, retention, and use, data access and third party transfers, restrictions on targeted advertising, and data deletion or disgorgement. In the context of AI chatbots, this may include limitations on how AI systems can store, partition, or use "memories" both within and across user sessions.

Harm Prevention Requirements
Data Collection and Minimization
Limits on Data Collection, Retention, and Use: Remedies should establish limits on data collection, retention, and use, and, where appropriate, include requirements for data destruction.
Restrictions on Data Access and Transfers: Remedies should establish permissible uses of data and require internal data access controls limited to approved use cases.
Restrictions on Targeted Advertising: Remedies should prohibit the collection and use of minors' personal data for targeted advertising.
Data Deletion and Disgorgement: When companies collect data unlawfully, remedies should specifically require data deletion or disgorgement of wrongful benefits.

1. Limits on Data Collection, Retention, and Use

Remedies should establish limits on data collection, retention, and use, and, where appropriate, include requirements for data destruction.

a. Data Collection

Limiting what data can be collected is a direct way to promote safer experiences. Enforcement agencies and legislators have increasingly required companies to justify their data collection, and have established stricter requirements related to data from minors. Data collection limitations can protect user privacy and limit the ability of social media and AI chatbot companies to leverage personal data to tailor recommendations and responses in ways that are harmful to vulnerable individuals.

Existing remedies establish limits on data collection. FTC remedies have required commitments from defendants to cease data-collection practices that undermine user privacy. Historically, this has included data gathered through online advertising auctions[43] as well as asking for users' passwords to

[42] Stipulated Order for Permanent Injunction and Civil Penalty Judgment, United States v. Epic Games, Inc., No. 5:22-cv-00518-BO (E.D.N.C. Feb. 7, 2023)
[43] Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025).

third-party websites.[44] FTC remedies have also considered how to restrict data collection to purposes necessary to operate the relevant product.[45]

b. Retention and Internal Use

Collecting less data is only part of the solution. When data is collected, companies should retain and use it in ways that align with remedy goals. Retention limits and use restrictions work together to ensure that data gathered for one purpose cannot quietly be repurposed, sold, or held indefinitely.

FTC data privacy and security remedies, as well as Illinois Biometric Information Privacy Act (BIPA) settlements, have required defendants to establish and maintain a data retention schedule that specifies a timeframe for the deletion of collected consumer information.[46] Defendants may commit to a timeframe that is reasonable and not indefinite.[47] In some remedies, companies have made more specific commitments, for example agreeing to retain data for the period necessary to fulfill the purposes of data collection.[48]

FTC remedies also limit how companies may use user data, including prohibition of the sale or use of sensitive categories such as health or precise location data. FTC remedies have included injunctions against disclosing or selling specific categories of data to third parties or for advertising purposes.[49] The FTC has prohibited internal uses of sensitive location data that link individual consumers to locations such as medical offices or religious institutions.[50]

Remedies have also sought to increase user control over permissible data use. These remedies are discussed in the Harm Mitigation section.

[44] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019).
[45] Proposed Modified Decision and Order, Facebook, Inc., FTC Docket No. C-4365 (May 3, 2023).
[46] *E.g.*, Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. June 22, 2023).
[47] *E.g.*, Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023).
[48] *E.g.*, Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief Against Defendant Cerebral, Inc., United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Amazon.com, Inc., No. 2:23-cv-00811-TL (W.D. Wash. July 19, 2023).
[49] *E.g.*, Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. June 22, 2023); Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief Against Defendant Cerebral, Inc., United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024); Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023).
[50] Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025); Decision and Order, InMarket Media, LLC, FTC Docket No. C-4803 (Apr. 29, 2024). Both of these settlements mandate a "sensitive location data program" with measures and policies to ensure that sensitive location data is not used in ways contrary to the settlement.

2. Restrictions on Data Access and Transfers

Remedies should establish permissible uses of data and require internal data access controls limited to approved use cases.

How companies collect, store, share, and use personal data is a central theme of technology regulation and enforcement. Restrictions on data access and transfer address two distinct but related problems, namely the risk that data is accessed or misused internally and the risk that it is shared with or exploited by third parties in ways that harm users. The FTC and Europe's General Data Protection Regulation (GDPR) enforcement have played an important role in catalyzing corporate privacy governance, including impacts on norms related to permissible data use.[51] Research suggests that relying on users to enforce their own data rights has had limited impacts and effective data controls are necessary.[52]

Many FTC remedies introduce expectations for data access controls and other measures to protect data security. Companies have agreed to limit employee and contractor access to personal information to what is necessary to perform their job functions.[53] Other remedies have included more detailed technical requirements related to privacy and data security, such as authentication and security protocols,[54] requirements to encrypt user data,[55] or multi-factor authentication for both employees and users.[56]

Remedies have also established standards for permissible sharing or selling data with third parties.[57] A settlement with Facebook, for example, secured declaratory relief from the company stating that it ceased specific third-party data-sharing practices.[58] FTC remedies have prohibited the sale, sharing, and disclosure of sensitive location data.[59]

Where companies share data with third parties, settlements have also required defendants to monitor the practices of third-party service providers, vendors, and customers who have access to user data. This included vetting parties before contracting with them, contractually obligating them to maintain

[51] Bamberger and Mulligan, "Privacy on the Book and on the Ground."
[52] Potter et al., "The Gap Between Data Rights Ideals and Reality."
[53] Stipulated Order for Injunction and Monetary Judgment, Fed. Trade Comm'n v. Ring, No. 1:23-cv-01549 (D.D.C. June 16, 2023); Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023).
[54] *E.g.*, Decision and Order, Zoom Video Communications, Inc., FTC Docket No. C-4731 (Jan. 19, 2021); Decision and Order, Drizly, LLC, FTC Docket No. C-4780 (Jan. 10, 2023); Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief Against Defendant Cerebral, Inc., United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024); Decision and Order, GoDaddy, Inc., FTC File No. 202-3133 (May 21, 2025).
[55] *E.g.*, Decision and Order, Support King, LLC, FTC Docket No. C-4756 (Dec. 21, 2021); Decision and Order, Zoom Video Communications, Inc., FTC Docket No. C-4731 (Jan. 19, 2021); Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief Against Defendant Cerebral, Inc., United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024).
[56] *E.g.*, Decision and Order, Drizly, LLC, FTC Docket No. C-4780 (Jan. 10, 2023); Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Twitter, Inc., No. 3:22-cv-03070-TSH (N.D. Cal. May 26, 2022); Decision and Order, GoDaddy, Inc., FTC File No. 202-3133 (May 21, 2025).
[57] See Nguyen et al., *Remedies for Tech-Related Harms Chapter 2*.
[58] Order Granting Final Approval to Class Action Settlement as Modified, Campbell v. Facebook, Inc., No. 4:13-cv-05996-PJH (N.D. Cal. Aug. 18, 2017).
[59] Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025); Decision and Order, InMarket Media, LLC, FTC Docket No. C-4803 (Apr. 29, 2024).

specific safeguards, or requiring self-certifications.[60] Some defendants also agree to audit the policies and practices of relevant third parties,[61] and a small number agree to train contractors or service providers as part of their compliance training programs.[62]

3. Restrictions on Targeted Advertising

Remedies should prohibit the collection and use of minors' personal data for targeted advertising.

Limiting how platforms can use personal data for advertising is a direct way to reduce incentives for harmful data collection and product design. Social media and AI chatbot companies' business models may depend on extending user engagement to maximize opportunities for data collection and targeted advertising. Prohibiting targeted advertising for minors addresses this dynamic at its source, by removing the financial incentive to surveil minors, profile their behavior, and design features to extend their use. Remedies should prohibit the collection and use of minors' personal data for targeted advertising purposes.

Within the context of AI chatbots, this may entail placing limits or restrictions on when or how personalized features of the AI system can be used to tailor, frame, or present ads to minors.[63] For example, remedies could restrict or prevent the use of within-session personalization (i.e., "short-term memory"), persistent, between-session personalization (i.e., "long-term memory"), user-specific knowledge bases, or user modeling to determine which ads to serve to minors or to tailor responses that serve those ads. Remedies could also prevent AI systems from storing information about minors specifically for the purposes of personalizing ads.

Existing remedies have restricted advertising practices and provide a foundation to build from. Google settled claims alleging that YouTube tracked and collected personal data about children under the age of 13 without parental consent.[64] Disney similarly settled claims with the FTC alleging that the company allowed YouTube to collect personal data from children without parental consent.[65] A settlement with Meta under the Fair Housing Act prohibits the use of particular forms of advertising, and requires Meta to notify the Department of Justice (DOJ) before adding new targeting options

[60] *E.g.*, Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief Against Defendant Cerebral, Inc., United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024); Decision and Order, GoDaddy Inc., FTC File No. 202-3133 (May 21, 2025); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. June 22, 2023).
[61] *E.g.*, Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025); Decision and Order, InMarket Media, LLC, FTC Docket No. C-4803 (Apr. 29, 2024) ; Stipulated Order for Permanent Injunction and Other Relief, Fed. Trade Comm'n v. Rite Aid, No. 2:23-cv-5023 (E.D. Pa. Feb. 26, 2024).
[62] *E.g.*, Decision and Order, GoDaddy Inc., FTC File No. 202-3133 (May 21, 2025); Decision and Order, Drizly, LLC, FTC Docket No. C-4780 (Jan. 10, 2023).
[63] See Bogen and Sampson, *It's (Getting) Personal*.
[64] YouTube Privacy Settlement, "Hubbard v. Google."
[65] Federal Trade Commission, "Disney to Pay $10 Million to Settle FTC Allegations the Company Enabled the Unlawful Collection of Children's Personal Data."

available for advertisers.[66] In the context of youth-targeted marketing, a JUUL settlement requires the company to refrain from advertising that directly or indirectly targets minors.[67]

4. Data Deletion and Disgorgement

When companies collect data unlawfully, remedies should specifically require data deletion or disgorgement of wrongful benefits.

Deletion and disgorgement remedies account for past violations while preventing future harms. They work to ensure that unlawfully obtained data cannot continue to be used, monetized, or built upon. In implementing this remedy, litigators should consider whether researchers should be able to analyze relevant data prior to deletion. This could be operationalized through disabling developer access or through maintaining the ability of users to download relevant data prior to deletion, which could then be shared through data donations, discussed in the Governance section.

FTC privacy and data security settlements include mandates for deletion or deidentification of unlawfully obtained data, with special rules for children. FTC remedies have required companies to delete personal information that was allegedly unlawfully obtained or otherwise implicated by the company's unlawful practices. Where the FTC alleges Children's Online Privacy Protection Rule (COPPA) violations related to parental consent or notice, settlements typically require children's data to be deleted unless the defendant obtains verifiable parental consent to retain it.[68] Similar deletion remedies extend beyond COPPA to broader FTC privacy remedies,[69] sometimes including deidentification as an alternative to outright deletion.[70]

Disgorgement remedies have taken several forms. A Facebook settlement required deletion of all cookie data collected from users who visited non-Facebook websites that used the Facebook Like button.[71] A settlement with Thomson Reuters required destruction of data from California residents who requested it.[72]

Such remedies are particularly relevant for AI chatbot companies. The FTC's remedy with Rite Aid, for example, required deletion of both images collected through its facial recognition system and any

[66] United States Department of Justice, "Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising."
[67] Final Consent Judgment, Commonwealth v. JUUL Labs, Inc., No. 200200962 (Pa. Ct. Com. Pl. Dec. 8 2022).
[68] *E.g.*, Stipulated Order for Permanent Injunction and Civil Penalty Judgment, United States v. Kuuhuub Inc., No. 1:21-cv-01758 (D.D.C. July 21, 2021); Stipulated Order for Permanent Injunction and Civil Penalty Judgment, United States v. Epic Games, Inc., No. 5:22-cv-00518-BO (E.D.N.C. Feb. 7, 2023).
[69] *E.g.*, Stipulated Order for Permanent Injunction and Other Relief, Fed. Trade Comm'n v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Pa. Feb. 26, 2024); Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief, United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024); Decision and Order, Drizly, LLC, FTC Docket No. C-4780 (Jan. 10, 2023); Decision and Order, Support King, LLC, FTC Docket No. C-4756 (Dec. 20, 2021).
[70] *E.g.*, Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025); Decision and Order, InMarket Media, LLC, FTC Docket No. C-4803 (Apr. 29, 2024).
[71] Class Action Settlement Agreement and Release, *In re* Facebook Internet Tracking Litigation, No. 5:12-md-02314-EJD (N.D. Cal. Feb. 14, 2022).
[72] Class Action Settlement Agreement, Brooks v. Thomson Reuters Corp., No. 3:21-cv-01418-EMC (N.D. Cal. Aug. 29, 2024).

algorithms or other products developed using those images.[73] Such an approach has been used in several settlements since the FTC's 2019 Cambridge Analytica case.[74]

In cases where the unlawful data practices included transfers to third parties, remedies can require companies to instruct those third parties to delete relevant data.[75] This typically requires written confirmation that those third parties have fulfilled the deletion mandate.[76]

Deletion and disgorgement remedies raise difficult questions of verification. It remains technically challenging to confirm that data or derived models have been fully destroyed, and enforcement agencies often lack the resources and technical capacity for granular auditing. These limitations underscore the importance of pairing deletion mandates with robust compliance mechanisms.

5. Remedy Not Included: Consent to Targeted Data Use

Remedies have sometimes required that platforms obtain express user consent before using or disclosing consumer data for advertising purposes, attempting to ensure that data collected in one context cannot be repurposed for commercial targeting without affirmative user agreement. FTC settlements with InMarket,[77] Twitter,[78] BetterHelp,[79] for example, require companies to obtain consent before using or disclosing user data to third parties for advertising.

Consent-based remedies, however, may have limited practical effect. Users already navigate a complex landscape of privacy choice online. The widespread reliance on user consent has produced what scholars describe as "consent fatigue,"[80] where ubiquitous consent prompts cause users to disengage from meaningful decision-making. Layering additional consent requirements onto targeted data use through remedy risks compounding this problem rather than solving it.

---

[73] Stipulated Order for Permanent Injunction and Other Relief at 12–13, Fed. Trade Comm'n v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Pa. Feb. 26, 2024)

[74] Final Order, *In re* Cambridge Analytica, LLC, FTC Docket No. 9383 (Nov. 25, 2019); see also Goland, "Algorithmic Disgorgement"; Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025); Decision and Order, InMarket Media, LLC, FTC Docket No. C-4803 (Apr. 29, 2024); Decision and Order, Avast Ltd., FTC Docket No. C-4805 (June 26, 2024); Stipulated Order for Injunction and Monetary Judgment, Fed. Trade Comm'n v. Ring LLC, No. 1:23-cv-01549 (D.D.C. June 16, 2023).

[75] *E.g.*, Decision and Order, FLO Health, FTC Docket No. C-4747 (June 22, 2021); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. June 22, 2023); Decision and Order, Avast Ltd., Docket No. C-4805 (June 26, 2024).

[76] *E.g.*, Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025).

[77] Decision and Order, InMarket Media, LLC, FTC Docket No. C-4803 (Apr. 29, 2024).

[78] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Twitter, Inc., No. 3:22-cv-03070-TSH (N.D. Cal. May 26, 2022).

[79] Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023).

[80] Schermer et al., "The crisis of consent"; Jones, *The Character of Consent*.

6. Remedy Not Included: User Controls for Data Sharing

At present, companies broadly determine how and when to share user data with third parties, with users having limited ability to meaningfully understand or control that process. Some remedies have sought to shift that balance by enabling users to assert greater control over how their personal data is used and disclosed, typically through opt-out mechanisms or express consent requirements. Because of the "consent fatigue" dynamic described above, however, opt-out and consent-based mechanisms for data sharing controls are unlikely to be effective for most users, and should not be relied upon as a primary remedy.

Some remedies have relied on user engagement to influence how data is shared. The Clearview AI settlement created an opt-out program for Illinois residents to block their faces from Clearview's search results, with Clearview required to advertise the program's availability.[81] FTC remedies have similarly included requirements for express user consent prior to the disclosure of consumer information to third parties.[82]

C. Age Assurance

Harm Prevention Requirements
Age Assurance
Age Assurance Safeguards: Where remedies require the company to provide specific protections to users based on their age, they should also require that the age assurance mechanisms the company adopts follow best practices for preserving privacy, accessibility, and efficacy.

Where remedies require the company to provide specific protections to users based on their age, they should also require that the age assurance mechanisms the company adopts follow best practices for preserving privacy, accessibility, and efficacy.

Age assurance remedies have taken several forms. Some remedies require assurance as a condition of data retention. For example, some remedies have required platforms to perform age assurance or obtain verifiable parental consent before retaining data previously collected from users.[83] Others focus on applying safer default settings for minors. A remedy with Epic Games, for example, required default settings that block disclosure of minors' personal information unless a parent or the user affirmatively consents, thereby placing the burden on the platform to protect minors rather than on families to opt

[81] See ACLU, "In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law."
[82] Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023); Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief Against Defendant Cerebral, Inc., United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024); Stipulated Order for Permanent Injunction, Monetary Judgment, and Other Relief, Fed. Trade Comm'n v. Voyager Digital, LLC, No. 1:23-cv-08960 (S.D. N.Y. June 27, 2025).
[83] *E.g.*, Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, United States v. Musical.ly, No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019); Stipulated Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief, Fed. Trade Comm'n v. NGL Labs, LLC, No. 2:24-cv-5753 (C.D. Cal. July 9, 2024).

in.[84] Age verification has also been required at the point of sale, as in the JUUL settlement, which mandated verification on websites and for all sales transactions.[85]

Age assurance remedies may be difficult to implement effectively and may introduce unintended negative impacts for both minor and adult users, including privacy risks and barriers to access.[86] Any age assurance or verification requirements included in remedies must account for these tradeoffs, weighing potential harms against the expected benefits for a given use case (e.g., restricting access to adult websites versus imposing safer default settings on social media). In addition, some percentage of minors will invariably circumvent age assurance requirements. As such, age assurance remedies must be paired with additional harm prevention and mitigation remedies.

To reduce the likelihood that the age assurance process itself poses undue risks to users, age assurance requirements imposed through remedies must include comprehensive safeguards for protecting users' privacy and preserving access, following prevailing industry best practices.

Because age assurance technologies and implementation approaches are still evolving, best practices related to efficacy, accessibility, privacy protection, and resistance to circumvention will continue to develop over time. Legal remedies should therefore be flexible and responsive to advances in both technical capabilities and governance frameworks. Yet at present, there is emerging work to define the core components of a high-quality age assurance system. Standards-setting bodies such as the International Organization for Standardization (ISO)[87] and the Institute of Electrical and Electronics Engineers (IEEE)[88] have begun to articulate high-level quality criteria for both system design and evaluation. These and other bodies may continue to develop and share recommendations that reflect prevailing consensus about industry best practices.[89]

One example of an existing best practice is support for multiple age signals. No single age assurance method will work effectively for all users. High-quality systems should therefore support multiple methods for demonstrating age and allow users to choose among them, including options that are more privacy-preserving. Moreover, systems should include fallback mechanisms when a given method fails or produces a low-confidence result. These design choices are critical because different methods perform unevenly across contexts and populations.[90]

---

[84] Stipulated Order for Permanent Injunction and Civil Penalty Judgment, United States v. Epic Games, Inc., No. 5:22-cv-00518-BO (E.D.N.C. Feb. 7, 2023); Stipulated Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief, Fed. Trade Comm'n v. NGL Labs, LLC, No. 2:24-cv-5753 (C.D. Cal. July 9, 2024).

[85] Consent Judgment, State ex rel. Jennings v. JUUL Labs, Inc., No. 2022-1137 (Del. Ch. Dec. 8, 2022).

[86] Rescorla et al., *Age Assurance Online*.

[87] International Organization for Standardization, "ISO/IEC 27566-1:2025."

[88] Institute of Electrical and Electronics Engineers, "IEEE Standard for Online Age Verification."

[89] KGI has published an extensive technical analysis of existing age assurance technologies, which can serve as a reference resource and a foundation for developing best practices and policies that stem from them. See Rescorla et al., *Age Assurance Online*.

[90] For example, facial age estimation systems may struggle to distinguish users near an age threshold, such as differentiating a 12-year-old from a 13-year-old, and methods that rely on government-issued identification or bank transactions may exclude users who do not have access to such credentials. Certain age assurance techniques, such as those relying on facial analysis, may also perform worse on users from certain racial or ethnic backgrounds, raising concerns about bias. See Children and Screens et al., "Comments to the Office of the New York State Attorney General on the Proposed Rules for the SAFE for Kids Act."

Current best practices for evaluation also underscore the importance of assessing the types of errors these systems can produce. This includes measuring both how often underage users are incorrectly granted access to restricted services and how often adults are wrongly denied access. Evaluating only one type of error risks producing systems that are either ineffective or overly exclusionary.[91] Assessing both types of error allows stakeholders to decide how to make tradeoffs as to which types of error are most important to address.

Privacy protections are a core component of high-quality age assurance systems. Where age assurance requires the collection of personal data and that data cannot be fully protected through technical guarantees, best practices include limiting data collection to what is strictly necessary, retaining it only for the duration required to complete the age assurance process, deleting it using industry-standard methods, and prohibiting its use for any secondary purposes such as sale, sharing, or user profiling.[92]

IV. Harm Mitigation Remedies

Harm mitigation remedies are measures that give users tools to report, avoid, or respond to harmful experiences with social media and AI chatbot companies.

Harm mitigation remedies rely on proactive user engagement rather than structural or default changes to product design. As a result, they generally seek to address harm after the fact rather than preventing it at the source. This section describes harm mitigation remedies in three areas: **product controls**, **user data controls**, and **reporting and removal**.

Harm mitigation tools broadly allow for individuals to report illegal content, adjust settings, or take other steps to actively avoid harmful experiences. This reliance on proactive user engagement is a limitation of mitigation-focused approaches. They generally respond to harm after it occurs or depend on user action to prevent it, rather than addressing the structural conditions that allow harm to arise in the first place. Company responses to user reporting are also uneven, with reports finding that some companies ignore or incorrectly reject a significant majority of user reports.[93]

[91] For an in-depth discussion of accuracy evaluation approaches, see Rescorla and Cooper, “First Steps Toward Operationalizing Age Assurance Mandates.”

[92] See, for example, Electronic Privacy Information Center, “EPIC’s Model Age-Appropriate Design Code (AADC) Model Legislation.”

[93] For example, reporting by Reuters suggests that Meta has historically acted on just 4% of the roughly 100,000 legitimate weekly fraud reports submitted by Facebook and Instagram users, ignoring or incorrectly rejecting the rest. Horwitz, “Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show.”

A. Product Controls

The remedy should require that social media and AI chatbot companies afford users with effective product controls to shape their user experience. Remedies should enable users to control their experience, report and avoid negative experiences, block unwanted contact, and limit time spent.

Harm Mitigation Requirements
Product Controls
User Controls: Remedies should require platforms to provide accessible and effective user safety, privacy, and time management tools.
Parental Controls: Remedies should require platforms to provide easily accessible and effective parental control tools for guardians of minors.

1. User Controls

Remedies should require platforms to provide accessible and effective user safety, privacy, and time management tools.

Remedies should require platforms to provide users with clear, easy-to-use options to indicate the experiences they want and those they wish to avoid, and to honor those preferences.[94] User-facing tools that are technically available but functionally ineffective provide little safety. A control buried in a settings menu, written in technical language, or requiring multiple steps to activate may exist in principle while remaining inaccessible in practice.

The remedy should therefore require companies to affirmatively demonstrate the effectiveness of user control features, not merely their existence. Platforms should be required to communicate clearly how each tool can be used to concretely reduce identified risks, and to show that users, particularly those users who experience harms alleged in litigation, can actually locate, understand, and deploy the tool. Effectiveness should be assessed through outcome-based metrics, such as whether users who engage with a control experience measurable reductions in the harm it is designed to address, rather than through simple disclosure that the feature exists.

Mandated user controls have taken several forms in existing remedies and provide a foundation to build from. In the security context, the Twitter settlement required the platform to offer specific forms of multi-factor authentication, illustrating that remedies can prescribe particular protective features rather than leaving design choices entirely to platforms.[95] A settlement with Zoom required extensive

[94] Moehring et al., *Better Feeds*; USC Marshall Neely Center for Ethical Leadership & Decision Making, “Neely Center Design Code for Social Media.”
[95] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Twitter, Inc., No. 3:22-cv-03070-TSH (N.D. Cal. May 26, 2022).

design changes to give users greater control over their security settings, demonstrating that courts can mandate functional redesign to increase safety.[96]

2. Parental Controls

Remedies should require platforms to provide easily accessible and effective parental control tools for guardians of minors.

Parental controls are only effective if parents and guardians can actually use them. Research shows that the effectiveness of parental control features is dependent on parental involvement, the technical capabilities of parents and guardians, as well as a parent's motivations for activating the tools.[97] Platform design choices significantly impact necessary technical skills and motivations. A parental control feature that exists in theory but cannot be found or configured in practice offers no meaningful protection. Remedies should therefore require platforms to provide parental management tools that are intuitive, simple, and accessible without specialized knowledge or significant time investment.

Beyond usability, remedies should address the structural problem of opt-in design. When parents and guardians must affirmatively select every individual safeguard, including account visibility, location accessibility, or contact availability, the burden falls on families rather than companies. Remedies should require default privacy-protective designs from the outset, so that the safest settings are active by default and parents are empowered to adjust them where necessary. A safe default experience is particularly important given the consent fatigue dynamic described above, which also applies to parents navigating product settings.

Remedies should also be designed to remain effective over time. Feature updates, interface redesigns, or new features can render existing parental controls obsolete or harder to access. Remedies should therefore include ongoing obligations, requiring platforms to maintain the accessibility and effectiveness of parental tools as their products evolve. Parental control features should be assessed through outcome-based metrics, for example measurable levels of efficacy (the experiences parents intend to restrict actually are restricted), parental satisfaction, and parental comprehension.

Existing remedies provide a foundation to build from. FTC orders regularly enforce COPPA compliance, including verifiable parental consent before collecting data from children.[98] These cases establish the principle that platforms must account for parental preferences and unique characteristics of minors. New remedies with social media and AI chatbot companies should extend and strengthen this principle and move beyond consent requirements to mandate easily accessible and effective parental control tools.

---

[96] Class Action Settlement Agreement and Release, *In re* Zoom Video Communications Inc., Privacy Litigation, No. 5:20-cv-02155-LHK (N.D. Cal. July 31, 2021).
[97] Stoilova et al., "Do Parental Control Tools Fulfil Family Expectations for Child Protection?"
[98] Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, United States v. Musical.ly, No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019); Stipulated Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief, Fed. Trade Comm'n v. NGL Labs, LLC, No. 2:24-cv-5753 (C.D. Cal. July 9, 2024); Stipulated Order for Permanent Injunction and Civil Penalty Judgment, United States v. Kuuhuub Inc., No. 21-cv-01758 (D.D.C. July 21, 2021).

B. User Data Controls

Remedies should require social media and AI chatbot companies to provide users with accessible, effective controls over their accounts and personal data, and to respect those choices in practice.

Harm Mitigation Requirements
User Data Controls
Account and Data Deletion: Remedies should require platforms to provide users with accessible tools to delete or deactivate their accounts and their associated data.
Data Portability: Remedies should require platforms to enable data portability, giving users meaningful ability to export their data.

1. Account and Data Deletion

Remedies should require platforms to provide users with accessible tools to delete or deactivate their accounts and their associated data.

Platform companies have historically made it easy to sign up and difficult to leave.[99] Remedies should require user-friendly account deletion or deactivation, changing existing processes that hide cancellation options, require a multitude of steps, or impose waiting periods designed to discourage follow-through.

Existing remedies provide instructive models. The FTC settlement with Vonage required implementation of a simple cancellation process, directly addressing the practice of making departure difficult.[100] The FTC's Amazon settlement required the platform to provide accessible mechanisms for users and parents to submit deletion requests.[101] Remedies in the gambling context have required platforms to provide self-exclusion options that disable the player's account(s) upon user request.[102] Taken together, these remedies establish the principle that the ease of exit should be commensurate with the ease of entry and that platforms should not be permitted to use friction as a tool for retaining users against their expressed wishes.

[99] Federal Trade Commission, *Bringing Dark Patterns to Light*.
[100] *See* Stipulated Order for Permanent Injunction, Monetary Judgment, and Other Relief, Fed. Trade Comm'n v. Vonage Holdings Corp., No. 3:22-cv-6435 (D.N.J. Nov. 3, 2022); Federal Trade Commission, "FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service."
[101] Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Amazon.com, Inc., No. 2:23-cv-00811-TL (W.D. Wash. July 19, 2023).
[102] Class Action Settlement Agreement at 18–19, Heathcote v. Spinx Games, No. 2:20-cv-01310-RSM (W.D. Wash. Feb. 15, 2022). See Responsible Gambling Council, "Looking to take a break from gambling?"

2. Data Portability

Remedies should require platforms to enable data portability, giving users meaningful ability to export their data.

At present, users who wish to leave a social media platform generally cannot take their data with them in any practical sense. A user's posts, connections, history, and preferences often remain locked within a single social media platform's systems. Data portability requirements can address this directly by ensuring that users can export their data in usable formats. Data portability can reduce switching costs that lock users into a specific provider even when they are dissatisfied or have experienced harm.

Data portability is not yet an established remedy in the US context. The FTC, for example, has not directly required data portability through existing consent decrees, but it has explored potential options to expand portability.[103] Utah has passed legislation establishing requirements for data portability, and there are additional proposals at the federal and state level.[104] These proposals provide users with the ability to both download their data and use it within applications that include data across platforms (interoperability). Interoperability can also provide users with more control over their user experience,[105] but such functionality needs to be designed carefully to avoid privacy issues.[106]

C. Reporting and Removal

Harm Mitigation Requirements
Reporting and Removal
User Reporting: Remedies should require effective user reporting mechanisms and concrete expectations for how platforms respond.

Remedies should require effective user reporting mechanisms and concrete expectations for how platforms respond.

Independent studies find that company reporting mechanisms fail users in two distinct ways: the tools are difficult to use, and users receive little or no meaningful feedback when they do report.[107] Studies find that many users, including minors, do not believe platforms will act on their reports at all.[108] Indeed, in 2022 Pew found that nearly three quarters of US teens thought social media sites were not doing enough to address online harassment.[109]

[103] Federal Trade Commission, "Data to Go."
[104] Hubbard, "Utah Digital Choice Act"; United States, "ACCESS Act."
[105] Open _Future, "_A Public, Interoperable Social Media Space."
[106] For example, the Cambridge Analytica scandal involved misuse of Facebook's interoperability APIs.
[107] See, e.g., Cover et al., "Reporting Online Abuse to Platforms"; Anti-Defamation League, *Block/Filter/Notify*.
[108] Vilk and Lo, *Shouting into the Void*.
[109] Vogels, *Teens and Cyberbullying 2022.*

The remedy should include concrete expectations for how social media and AI chatbot companies respond promptly and effectively to user reports. A settlement with Zoom, for example, requires the creation of a user-support ticket system for reports of meeting disruptions.[110] Reporting mechanisms should be accessible and intelligible to all users, particularly minors. Platforms should provide specific reporting tools but describe how these tools produce meaningful outcomes, including specific timelines, escalation processes, and follow-up to the reporting user.

V. Governance Remedies

Governance remedies are measures designed to influence how a company makes decisions, exercises leadership oversight, and enforces compliance specific to the remedies.

Governance remedies work to narrow opportunities for companies to make design decisions that harm consumers moving forward. For this reason, governance remedies should incorporate a combination of **internal governance requirements**, **independent monitoring**, and **transparency mechanisms**. This section articulates core requirements for remedies in each of these three areas.

Many FTC settlements have focused on company governance, often requiring the establishment of "comprehensive privacy programs" and "comprehensive internal security programs" overseen by senior officers, independent committees, or board level leadership.[111] These structures are designed to prevent companies from circumventing remedy goals and ensure that harmful practices are anticipated and prevented.

Some have questioned the effectiveness of standalone governance remedies, arguing that these remedies can "simply create box-checking exercises."[112] Indeed, following a remedy, there will undoubtedly be incentives for companies to sideline mandated governance mechanisms to avoid disruption to core business practices, while technically satisfying the terms of the remedy. As such, governance remedies should supplement additional harm prevention and mitigation remedies.

[110] Class Action Settlement Agreement and Release, *In re* Zoom Video Communications, Inc. Privacy Litigation, No. 5:20-cv-02155-LHK (N.D. Cal. July 31, 2021).
[111] Examples of more individualized programs include Rite Aid 2024's "comprehensive…monitoring program" to oversee and audit the policies and procedures governing the use of any automated biometric security or surveillance system using consumer biometric data, and MyLife 2024's "FCRA monitoring program" to govern any activities that involve selling consumer information. *See* Stipulated Order for Permanent Injunction and Other Relief, Fed. Trade Comm'n v. Rite Aid, No. 2:23-cv-05023-KBH (E.D. Pa. Feb. 26, 2024); Stipulated Order for Permanent Injunction and Equitable Monetary Relief, United States v. MyLife.com, No. 2:20-cv-06692-JFW (C.D. Cal Dec. 15, 2021).
[112] Jerome, "Can FTC Consent Orders Effectively Police Privacy?"

A. Internal Governance Requirements

Remedies should require that companies establish or designate specific compliance mechanisms to oversee remedy compliance, including by updating employee performance and compensation structures that are misaligned with remedy goals. For example, an organization or team's bonuses should not be tied to metrics that correlate with harms relevant to litigation.

Governance Remedies
Internal Governance Requirements
Compliance Officer: Remedies should require the company to designate a senior-level compliance officer, supported by a cross-functional committee, responsible for ensuring and embedding compliance across all elements of the remedy.
Organizational Goals: Remedies should require the company to ensure that product, performance, and compensation goals and implementation structures align with remedy goals.

1. Compliance Officer

Remedies should require the company to designate a senior-level compliance officer, supported by a cross-functional committee, responsible for ensuring and embedding compliance across all elements of the remedy.

A compliance officer is necessary for ensuring a single, consistent focal point that ensures remedy compliance across the company. This official should be responsible for coordinating internal governance processes necessary for fulfilling compliance at all levels.

Compliance mechanisms are commonly integrated into remedies across sectors. Remedies regularly require the establishment or designation of a specific company compliance officer,[113] internal compliance oversight committee or function,[114] and/or a specific board compliance committee.[115]

None of these mechanisms are a silver bullet for changing corporate conduct to align with remedy goals. Where remedies conflict with short-term corporate financial interests, such as by requiring changes to engagement-maximizing design features that contribute to advertising revenue, companies

[113] *See*, *e.g.*, Final Consent Judgment, Commonwealth v. JUUL Labs, Inc., No. 200200962 (Pa. Ct. Com. Pl. Dec. 8, 2022); Decision and Order, Facebook, Inc., FTC Docket No. C-4365 (Aug. 10, 2012).
[114] Shen, *National Opioid Litigation* requires the establishment of an opioid-focused internal Controlled Substance Monitoring Program (CSMP) committee. In the civil rights context, settlements have required the establishment of internal compliance mechanisms. *See*, *e.g.*, Settlement Agreement and Stipulated [Proposed Order] of Resolution, United States v. Seattle, No. 12-CV-01282 (W.D. Wash. July 27, 2012); Settlement Agreement and Order, United States v. East Haven, 3:12-cv-01652-AWT (D. Conn. Nov. 20, 2012); Consent Agreement, United States v. Miami-Dade County, No. 1:13-cv-21570-XXXX (S.D. Fla. May 1, 2013).
[115] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019). The FTC's majority statement said that this remedy was designed to help limit Mark Zuckerberg's ability "to make privacy decisions unilaterally." Federal Trade Commission, "Statement of Chairman Joe Simons."

have incentives to circumvent governance constraints. A governance mechanism focused on decreasing time spent on social media or AI chatbots, for example, could translate to reduced personal data collection or short-term revenue. For this reason, litigators should anticipate that companies may face competing priorities between existing corporate practices and remedy goals. Such challenges are compounded in technology companies, where formal governance structures have typically centralized authority with a small group of executives.[116] For these reasons, compliance mechanisms must be supported by additional strategies to ensure effective remedy governance.

2. Organizational Goals

Remedies should require the company to ensure that product, performance, and compensation goals and implementation structures align with remedy goals.

Ensuring that product, performance, and compensation goals are not misaligned with remedy goals is important for embedding governance across the company. Product, performance, and compensation goals are a critical governance mechanism at many technology companies. Organizational, team, and individual performance goals can be tied to individual compensation and bonus schedules. Remedies should require that company performance and compensation goals and metrics are not misaligned with remedial objectives.[117] For example, if a remedy seeks to prevent or mitigate harms from problematic use, it could end the use of performance metrics, financial incentives, and compensation that are specifically tied to a particular problematic feature designed to increase the prevalence of overnight use. The remedy could further require that the company document product team goals within the compliance function.[118]

Product, performance, and compensation goals could further integrate alternative metrics of user safety, wellbeing, and benefit.[119] As described within the measurement mandates section, product, performance, and compensation goals could move away from minimizing harms to instead maximizing long-term user value. Additional metrics could further ensure that teams and individuals tasked with safety work have compensation and promotion structures that are not only tied to overall product key performance indicators (KPIs).

While performance and compensation remedies do not regularly appear in publicly available technology remedies, remedies in other industries have targeted performance as a way to institutionalize remedy compliance. Settlements with the major pharmaceutical companies Janssen, Teva, Allergan, and Mallinckrodt require each company to end compensation structures and incentives tied to increasing the volume of opioid sales.[120] Given that opioid sales volume can raise risks of dependence or addiction, parallels can be drawn to goals related to promoting habitual use in social

[116] Leerssen, "From Murdoch to Musk."
[117] See Atabey et al., *Children & AI Design Code* suggesting an "executive leadership" with authority and responsibility to set company-wide incentives and performance metrics; approve, delay, or block product launches; and assume ultimate accountability for risk-based design and deployment decisions.
[118] Lubin et al., "Social Media Harm Abatement."
[119] Moehring et al., *Better Feeds*.
[120] Shen, *National Opioid Litigation*.

media and AI chatbot litigation.[121] As such, internal governance remedies can include a focus on eliminating organizational, team, and individual goals related to the harmful practices at issue in litigation as well as the integration of goals focused on longer-term user value.

3. Remedy Not Included: Training Requirements

Training for employees, typically on an annual basis, is a standard feature of FTC privacy and information security remedies. Training is sometimes required for all employees or it is mandated only for specific, relevant job functions.[122] Some settlements require that independent third parties certify training effectiveness.[123] While technology remedies have historically included staff-level training, these alone have not served to catalyze structural changes.[124] When considering potential remedies, policymakers and litigators should likely prioritize more impactful interventions.

B. Monitoring and Measurement

To support effective internal governance, the remedy should also require independent monitoring and measurement of compliance with related remedies. This should include the establishment of an independent monitor, as well as the introduction of specific measurement and transparency mandates.

Governance Remedies
Independent Monitoring
Independent Monitor: Remedies should establish an independent monitor to ensure compliance through a regular reporting schedule and periodic audits by qualified independent auditors.
Measurement Mandates: Remedies should require internal and external measurement and reporting of specific metrics responsive to the harms alleged in litigation.
Transparency Mechanisms: Remedies should require the establishment of a document repository for documents relevant to litigation as well as guarantee researcher access to data relevant to the harms alleged in litigation.

[121] *E.g.*, YouTube's 2018 goal to increase habitual users. Amended Ex. 701, Plaintiffs' Omnibus Opposition to Defendants' Motions for Summary Judgment, *In re* Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal. Feb. 20, 2026). And Meta: Amended Exhibit 15, Plaintiffs' Omnibus Opposition to Defendants' Motions for Summary Judgment, *In re* Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal. Feb. 20, 2026).
[122] *E.g.*, Stipulated Order for Permanent Injunction, Civil Penalty, and Other Relief, United States v. Easy Healthcare, No. 1:23-cv-3107 (N.D. Ill. June 22, 2023); Decision and Order, Mobilewalla, Inc., FTC Docket No. C-4811 (Jan. 13, 2025); Decision and Order, InMarket Media, LLC, FTC Docket No. C-4803 (Apr. 29, 2024).
[123] Memorandum Opinion and Order, *In re* TikTok, Inc., Consumer Privacy Litigation, No. 1:2020cv04699 (N.D. Ill. Jan. 25, 2024).
[124] De Mooy, "How to Strengthen the FTC Privacy & Security Consent Decrees." See also Bamberger and Mulligan, "Privacy on the Books and on the Ground."

1. Independent Monitor

Remedies should establish an independent monitor to ensure compliance through a regular reporting schedule and periodic audits by qualified independent auditors.

An independent monitor is critical for effectively supervising company compliance across harm prevention, mitigation, and governance. The independent monitor should be responsible for compliance and have the authority to conduct investigations, influence specific organizational measurement strategies, inspect internal records, supervise independent audits of relevant products and systems, and interview employees.

a. Establishing an Independent Monitor

An independent monitor should be structured as a standing body with a defined mandate, adequate resourcing, and a clear reporting relationship to the court or relevant authority. Its composition should be interdisciplinary and diverse, drawing on experts in technology, data science, law, health and wellbeing, education, or other fields relevant to the specific harms at issue in litigation.

Some technology remedies have required that companies maintain records and allow for the FTC or state attorneys general to request additional information without further court intervention.[125] Antitrust cases have required the parties to establish a technical committee, which is an independent body of experts responsible for supporting remedy implementation and compliance.[126]

Settlements with tobacco companies and law enforcement have established robust external mechanisms. In the case of tobacco settlements, a Master Settlement Agreement (MSA) designated the National Association of Attorneys General (NAAG) as a central monitoring mechanism, including the allocation of more than $50 million to support remedy compliance oversight.[127] The MSA imposes several requirements on tobacco companies including restrictions on advertising, eliminating practices that obscure the risks of tobacco usage, and raising the costs of cigarettes, all efforts to meet the MSA's stated goal of reducing smoking, especially among minors.[128]

Independent monitoring is a critical component of civil rights remedies involving law enforcement and corrections departments. In these cases, DOJ remedies have established interdisciplinary monitoring teams with broad authority as a way to encourage police reform.[129] Monitoring teams are selected after negotiations between parties and are typically composed of experts with relevant knowledge specific

---

[125] *See*, *e.g.*, Stipulated Order for Permanent Injunction, Monetary Judgment, and Other Relief, Fed. Trade Comm'n v. Voyager Digital, LLC, No. 1:23-cv-08960 (S.D. N.Y. June 27, 2025); [Proposed] Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm'n v. Ascend CapVentures, No. 2:24-cv-07660-SPG-JPR (C.D. Cal. June 23, 2025); Stipulated Order for Permanent Injunction, Monetary Judgment, and Other Relief, Fed. Trade Comm'n v. Empire Holdings Grp., LLC, No. 2:24-cv-04949-WB (E.D. Pa. May 8, 2025).
[126] See, e.g., Arnao et al., *Designing the Technical Committee for the United States v. Google Search Antitrust Remedy*.
[127] National Association of Attorneys General, "The Master Settlement Agreement."
[128] Ibid.
[129] *See*, *e.g.*, Consent Decree Monitor, "The Consent Decree"; Collaborative Agreement, *In re* Cincinnati Policing, No. C-1-99-317 (S.D. Ohio Apr. 11, 2002); United States Department of Justice, "Justice Department Secures Agreement with Cumberland County"; United States Department of Justice, "New Jersey Settles Allegations of Discrimination by State Police Under Justice Department Agreement."

to the specific case. They can include experts in police practices, accountability, community engagement, and data analysis. These professionals are paid, with their fees and costs generally covered by the defendant.[130] Monitoring teams are typically responsible for assessing compliance, conducting audits and investigations, reporting pertinent updates to the parties and the court, and, where relevant, providing technical assistance. Effectiveness of these mechanisms in the law enforcement context has been described as uneven, including whether the costs of such interventions lead to desired outcomes and the overall effect on the communities within which the monitoring is taking place.[131]

b. Reporting

The remedy should require company reporting to the independent monitor, on behalf of the court, as well as users and the broader public.

Reporting to the independent monitor will allow for structured reporting on remedy progress, including confidential information as necessary. FTC settlements often require a compliance report one year after the settlement's effective date,[132] and state attorneys general settlements also regularly involve some form of compliance reporting.[133]

In practice, compliance reports may become formulaic and difficult for the general public to decipher.[134] As such, in addition to reporting to the independent monitor, the company should also be required to publicly report on key indicators related to case-specific harms. This could obligate companies to either finance a third-party platform with specific expertise in the systems and harms at issue in litigation or maintain a company-developed public-facing platform interface that enables users, experts, and journalists to track and analyze key metrics. The use of a third-party platform must account for privacy and safety considerations. Previous remedies in some sectors have required reporting to the public. Within civil rights settlements, for example, there are examples of police departments agreeing to quarterly public reports on agreed indicators[135] as well as public-facing data dashboards.[136]

---

[130] *See*, *e.g.*, Settlement Agreement and Stipulated [Proposed Order] of Resolution, United States v. Seattle, No. 12-CV-01282 (W.D. Wash. July 27, 2012); Settlement Agreement and Order, United States v. East Haven, 3:12-cv-01652-AWT (D. Conn. Nov. 20, 2012); Consent Agreement, United States v. Miami-Dade County, No. 1:13-cv-21570-XXXX (S.D. Fla. May 1, 2013); United States Department of Justice, "Department of Justice and Montgomery County, Maryland enter into voluntary agreement addressing police practices."

[131] See Martinez, "Independent Monitorships."

[132] *See*, *e.g.*, Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm'n v. Next-Gen, Inc, No. 4:180CV-0128-DGK (W.D. Mo. Mar. 7, 2019); Decision and Order, Intellivision Technologies Corp., FTC Docket No. C-4809 (Jan. 8, 2025).

[133] *See*, *e.g.*, Final Stipulated Consent Judgment, State ex rel. Weiser v. JUUL Labs, Inc., No. 2020CV32283 (Colo. Denv. Cnty. Dist. Ct. Apr. 12, 2023).

[134] See, e.g., Jerome, "Can FTC Consent Orders Effectively Police Privacy?"

[135] *See*, *e.g.*, Consent Decree, United States v. Newark, No. 2:16-cv-01731-MCA-MAH (D.N.J. Oct. 6, 2017); United States Department of Justice, "Department of Justice and Montgomery County, Maryland enter into voluntary agreement addressing police practices."

[136] See Portland Police Bureau Office of the Inspector General, *PPB Force Analysis Annual Summary Report 2025*.

c. Auditing

The independent monitor should establish and supervise regular audits of remedy compliance. With social media and AI chatbot remedies, audits could encompass a range of activities to verify that self-reported compliance accurately reflects actual company behavior and user experience. Depending on the specific case, this could include review of internal testing records,[137] algorithmic systems, product decision-making documentation, or agreed upon metrics associated with specific products, features, or teams. Given the technical complexity of social media and AI chatbot products, and the pace at which companies update them, audits should be conducted by independent assessors with relevant technical expertise and should occur on a schedule tied to the company's product development cycles.[138] Where relevant auditing accreditations exist, the independent monitor may require auditors have relevant training, domain specific knowledge, and experience. Furthermore, auditors should not have any financial incentive to certify compliance, in order to ensure meaningful independence.

Remedies routinely require some form of auditing, but the substance, specific obligations, and timelines differ. FTC remedies have recently imposed biannual audits of remedy requirements.[139] In a class action settlement, Thomson Reuters agreed to "substantially increase" the number of its internal audits investigating compliance with product use under state and federal laws.[140] Similarly, settlements with the e-cigarette company JUUL required the company to conduct regular retailer inspections and internal audits.[141] Civil rights remedies require unannounced inspections and law enforcement integrity audits.[142] These audits can serve to inform the independent monitor's review of remedy compliance.

2. Measurement Mandates

Remedies should require internal and external measurement and reporting of specific metrics responsive to the harms alleged in litigation.[143]

Measurement mandates can serve as an important strategy to generate actionable, ongoing compliance data that confirms that remedy goals are being met.

a. Establishing a Measurement Mandate

Measurement mandates can help ensure that remedies meaningfully reduce risk and harm for users. Companies' own internal research and assessments, containing specific metrics linking specific design practices to user harms, are being used as evidence in lawsuits to demonstrate knowledge and, in some cases, intentionality. Given the increasing regulatory and legal risk associated with internal research examining design-based risks and harms, companies are actively ending investment

[137] See Lubin and Iyer, "How Tech Regulation Can Leverage Product Experimentation Results."
[138] See Lubin et al., "Social Media Harm Abatement."
[139] *See* Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, U.S. v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. June 22, 2023).
[140] Class Action Settlement Agreement, Brooks v. Thomson Reuters Corp., No. 3:21-cv-01418-EMC (N.D. Cal. Aug. 29, 2024).
[141] Consent Judgment, Commonwealth v. JUUL Labs, Inc., No. 2084CV00402 (Mass. Super. Ct. Apr. 12, 2023).
[142] *See* Consent Decree, United States v. City of Los Angeles, No. CV 00-11769 GAF (C.D. Cal. June 15, 2001).
[143] For a more detailed description of this remedy, see Lubin et al., "Social Media Harm Abatement."

in research as a way to reputational and legal risk.[144] Indeed, there are existing examples of companies and their lawyers instructing or advising internal company researchers to avoid research on particular topics, including in the context of tobacco litigation[145] as well as social media platforms.[146] Companies may alternatively simply choose to adopt metrics that include narrowly defined harms that do not fully account for potential risk.

As such, measurement mandates help ensure ongoing and effective internal company research that examines harm and wellbeing. Measurement mandates can help confirm the remedy is structured in a way that materially reduces risks over time. At the same time, measurement remedies will undoubtedly be harder to implement than remedies that require a company to cease a certain practice altogether or establish a specific governance structure. Implementation of such remedies is better suited to attorneys general and regulatory agencies than to private litigation, in light of the sustained oversight they require.

Measurement remedies have been used in litigation across sectors. Within the social media context, Meta has previously agreed to ongoing third-party assessments of metrics related to nondiscriminatory ad delivery.[147] FTC settlements have required specific measurement obligations, including in its settlement with Rite Aid where the company agreed to conduct and document annual testing to evaluate system accuracy and risk of demographic bias.[148] Settlements in other sectors also have ongoing testing and screening requirements.[149]

Social media and AI chatbot companies already track a range of relevant metrics, and the remedy can integrate into these existing structures.[150] However, existing metrics are often narrowly constructed to conform to individual platforms' definitions of harms, which makes them both unresponsive to many users' complaints as well as unable to be compared across platforms. The independent monitor should work with interdisciplinary experts to create standardized metrics that best reflect user concerns and that allow for cross-platform comparison.

[144] See United States Senate Judiciary Subcommittee on Privacy, Technology, and the Law, "Hidden Harms"; Moran et al., "The End of Trust and Safety?"
[145] Hanauer et al., "Lawyer Control of Internal Scientific Research to Protect Against Products Liability Lawsuits."
[146] United States Senate Judiciary Subcommittee on Privacy, Technology, and the Law, "Hidden Harms."
[147] See Guidehouse, *VRS Compliance Metrics Verification Report*; Austin, "An Update on Our Ads Fairness Efforts."
[148] Stipulated Order for Permanent Injunction and Other Relief, Fed. Trade Comm'n v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Pa. Feb. 26, 2024); *see also* Decision and Order, Zoom Video Communications, Inc., FTC Docket No. C-4731 (Jan. 19, 2021).
[149] See Shen*, National Opioid Litigation*.
[150] *E.g.*, documents released in the MDL: Partially Unsealed Meta Exhibits to Less Redacted Corrected Omnibus Opposition to Defendants' Motions for Summary Judgment, *In re* Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal. Jan. 20, 2026); Partially Unsealed TikTok Exhibits to Less Redacted Corrected Omnibus Opposition to Defendants' Motions for Summary Judgment, *In re* Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, No. 4:22-md-03047-YGR (N.D. Cal. Jan. 20, 2026).

b. Internal Measurement

Internal measurement is focused on operational and product decisions taken by the company.[151]

The remedy should introduce requirements for companies to track and report on design features and algorithmic processes identified as harmful. Measurement mandates should integrate specific obligations into existing product evaluation procedures.[152] Furthermore, the remedy should establish requirements that the platform retains records of testing that substantiate relevant product safety statements and, where relevant, reasons for not implementing alternative product designs or safeguards.[153]

Internal measurement should also require social media and AI chatbot companies to run universal holdout experiments – where a group of users is exempted from design changes for at least 12 months to demonstrate potential long-term user impacts of a particular product design choice.[154] This will enable assessment of the aggregate effects of a company's product decisions against a stable control group. Internal experimental protocols should also be required to incorporate intermediate indicators of harm, including user experience and behavioral risk factors that are predictive of longer-term health outcomes even where short-term metrics are insufficient to capture them.[155]

c. External Measurement

External measurement is focused on independent measurement of outcomes relevant to the case.[156]

The remedy should establish specific external measurement obligations that enable assessment of remedy progress over time. Measurement should be conducted through an independent, ongoing system for collecting data that does not depend on company access or collaboration. Such measurement would be independent from the company and offer an external check on its reporting from internal measurement.[157]

This should include independently administered longitudinal user surveys. These surveys could focus on general users or specific at-risk populations and allow for comparisons that enable assessors to benchmark on harm and wellbeing over time. This could focus on an individual platform, or potentially across multiple platforms, depending on the case. As a further accountability mechanism, the company should be required to facilitate independent researcher access to platform data, as described in the following Transparency Mechanisms section.[158]

---

[151] Lubin et al., "Social Media Harm Abatement."
[152] Lubin and Iyer, "How Tech Regulation Can Leverage Product Experimentation Results."
[153] *E.g.,* Decision and Order, BetterHelp, Inc., FTC Docket No. C-4796 (July 7, 2023); Decision and Order, Avast Ltd., FTC Docket No. C-4805 (June 26, 2024); Joint Stipulation for Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief, United States v. Cerebral, Inc., No. 1:24-cv-21376-JLK (S.D. Fla. Apr. 15, 2024); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, United States v. Amazon.com, Inc., No. 2:23-cv-00811-TL (W.D. Wash. July 19, 2023).
[154] Moehring et al., *Better Feeds*.
[155] For a discussion of an "Internal Mechanism," see Lubin et al., "Social Media Harm Abatement."
[156] Ibid.
[157] Ibid.
[158] Ibid.

Lastly, the remedy should establish a mechanism through which the company will fund the external mechanism. Funding should be managed in a way that ensures independence and prevents company oversight of the external mechanism's day-to-day work.

3. Transparency Mechanisms

Remedies should require the establishment of a document repository for documents relevant to litigation as well as guarantee researcher access to data relevant to the harms alleged in litigation.

Transparency mechanisms can expand the types of researchers and organizations that are able to analyze relevant company documentation at issue in litigation.

a. Document Repository

The remedy should require the creation of an independent, publicly accessible document repository that includes company documents relevant to the litigation. The company should fund an independent institution to host these documents. The remedy should define the scope of documents for inclusion, including in relation to privacy, trade secrets, and legal privilege. It should also establish a mechanism to efficiently resolve disputes around the inclusion of specific documents.[159] The remedy should spell out technical specifications for the independent document repository, including access eligibility as well as search and index capabilities.

Previous remedies created document repositories of documents produced through litigation to further accountability. The State of Minnesota's 1998 tobacco settlement created the Minnesota Tobacco Document Depository,[160] with the MSA building on this approach, and requiring that all original participating tobacco manufacturers[161] publicly disclose all internal, non-privileged documents[162] produced in smoking and health-related litigation. These documents are now hosted by the Legacy Tobacco Documents Library at the University of California, San Francisco (UCSF).[163] The UCSF industry archives library includes hundreds of publications across a range of disciplines which have relied on industry documents disclosed through the archive.[164] The World Health Organization has highlighted that the archive has served as a key tool for journalists, lawyers, and policymakers in the US and beyond.[165] The JUUL settlements adopted a similar approach, with state settlements requiring

[159] Final Stipulated Consent Judgment, State ex rel. Weiser v. JUUL Labs, Inc., No. 2020CV32283 (Colo. Denv. Cnty. Dist. Ct. Apr. 12, 2023).
[160] Settlement Agreement and Stipulation for Entry of Consent Judgment, Minnesota v. Philip Morris Inc., No. C1-94-8565 (Minn. Dist. Ct. May 8, 1998).
[161] The Original Participating Manufacturers in the MSA are Philip Morris USA, R.J. Reynolds Tobacco Company, Brown & Williamson Tobacco Corporation, and Lorillard Tobacco Company.
[162] See Hurt et al., "The Open Doorway to Truth."
[163] See University of California, San Francisco, "About the Truth Tobacco Industry."
[164] Ibid.
[165] World Health Organization, *The Tobacco Industry Documents*.

that a public university or research institution is designated to serve as a document repository for JUUL litigation documents.[166]

Settlement agreements with opioid companies also required the disclosure of relevant documents, including internal, non-privileged opioid-related industry documents.[167] These documents are now maintained by the UCSF-JHU Opioid Industry Documents Archive.[168]

b. Researcher Access

The remedy should require that companies take affirmative steps to enable independent researchers[169] to conduct research that is relevant to the harm at issue in the case. The remedy should describe specific steps companies are expected to take to enable this research, including access to publicly available platform data, through user data donations, or, in some circumstances, with privileged access to private platform data.[170]

The remedy should oblige companies to provide a safe harbor for researchers conducting relevant public interest research, subject to relevant privacy protections.[171] The safe harbor should prevent companies from taking legal action against independent researchers who rely on publicly available information or consensually provided user information, where specific privacy standards are upheld.[172] Independent research, conducted by academics, civil society organizations, and journalists, has contributed to our understanding of risks and mitigations in concrete ways.[173] The remedy should establish the conditions for this research focused on social media and AI chatbot companies. The remedy could further mandate Application Programming Interface (API) access for independent researchers conducting particular research related to relevant harms at issue in the litigation, particularly for specific populations such as minors.[174]

The remedy should also establish a dedicated funding mechanism to support research and testing of company systems. One model would require companies to contribute to a restricted trust fund, potentially structured through a *cy pres* arrangement, from which qualified nonprofit organizations and researchers could apply for resources to conduct safety research and auditing. Remedy funding of this kind would create an efficient and durable research infrastructure that does not depend on the goodwill or continued cooperation of the social media or AI chatbot companies themselves.

---

[166] *See* Final Consent Judgment, North Carolina v. JUUL Labs, Inc., No. 19CVS2885 (N.C. Super. Ct. June 28, 2021); *see also* Consent Judgment, Minnesota v. JUUL Labs, Inc., No. 27-CV-19-19888 (Minn. Dist. Ct. Hennepin Cnty. May 16, 2023); University of California, San Francisco, "Juul Labs Collection."
[167] Final Judgment, California v. McKinsey & Co., Inc., No. RG21087649 (Cal. Super. Ct. Alameda Cnty. Feb. 4, 2021); Consent Judgment, Massachusetts v. Publicis Health, LLC, No. 2184-CV-01055-BLS1 (Mass. Super. Ct. Suffolk Cnty. Jan. 31, 2024); Kroger Settlement Agreement, *In re* National Prescription Opiate Litigation, MDL No. 2804 (N.D. Ohio Mar. 22, 2024).
[168] University of California, San Francisco, "About OIDA."
[169] The term "independent researcher" is used broadly and intended to include academics as well as journalists and civil society organizations conducting research related to harms relevant to the litigation.
[170] See Abdo et al., *Better Access*.
[171] Longpre et al., "A Safe Harbor for AI Evaluation and Red Teaming"; Abdo et al., *A Safe Harbor for Platform Research*.
[172] See United States, "Platform Accountability and Transparency Act."
[173] See Shiffman and Silverman, *The Case for Transparency*.
[174] Nguyen et al., *AI Companions & Harms to Children*.

Precedents for transparency remedies exist across industries. The tobacco, JUUL, and opioid settlements each required the establishment of document repositories to facilitate external research. These settlements further required companies to fund specific public interest activities, including expenditures related to independent research. The tobacco MSA, for example, requires companies to fund efforts to decrease youth smoking and promote public health. It also prohibits industry agreements to limit or suppress research into tobacco and health.[175] DOJ consent decrees with law enforcement have also required proactive data access and research mechanisms.[176]

VI. Conclusion

The expanding body of litigation against social media and AI chatbot companies represents a pivotal moment for accountability. As cases advance to discovery and trial, courts are emerging as central actors in shaping technology policy. Court decisions – particularly at the remedy phase – will impact the design, governance, and accountability of social media and AI chatbot companies.

The ultimate outcomes of cases will depend on the remedies that are ordered. Monetary damages alone are unlikely to fundamentally change risk. As tobacco, opioid, and e-cigarette litigation has demonstrated, durable changes in company conduct typically also requires injunctive relief.

Designing Technology Remedies offers a practical, evidence-based framework to help litigators, courts, and policymakers identify and implement effective and enforceable remedies that are responsive to specific social media and AI chatbot harms. By organizing remedies into **harm prevention**, **harm mitigation**, and **governance**, the framework provides a structured, evidence-based approach to addressing the complex challenges raised by social media and AI chatbot products.

These categories are mutually reinforcing: preventing harm through safer design, equipping users to mitigate harmful experiences, and ensuring robust oversight and accountability mechanisms. Effective remedies will combine all three categories. Prevention, mitigation, and governance are mutually reinforcing and no single category is sufficient on its own for addressing harm.

The cases now moving through US courts – and the remedies they may produce – will have implications far beyond the parties involved. They will catalyze future litigation, inform regulatory approaches to platform governance, and help to shape technology policy in the US and globally. Litigation presents a critical opportunity to translate available research and evidence into durable, enforceable change.

Designing Technology Remedies seeks to meet this moment by providing practical, evidence-based tools for crafting remedies that place user safety and well-being at the center, while effectively addressing harms associated with social media and AI chatbot companies.

---

[175] Master Settlement Agreement, Mississippi v. Philip Morris Inc., No. 94-1429 (Nov. 23, 1998).
[176] Consent Decree, United States v. Newark, No. 2:16-cv-01731-MCA-MAH (D.N.J. Oct. 6, 2017).

Appendix A. Methodology

In 2025, KGI, TJL, and the USC Neely Center analyzed nearly 100 judicial and settlement remedies relevant to digital platform and social media litigation.[177] These include remedies from FTC consent decrees, technology, gambling, public health, and public interest litigation. Research focused on injunctive relief across a spectrum of potential remedy interventions relevant to digital platforms, including governance, harm prevention, and mitigation. Desk research was supplemented by select interviews with attorneys, experts, and researchers involved in complex cases. Interviews revealed lessons and effective practices for crafting remedies that respond to complex harms, including in relation to social media and AI chatbot companies.

In late 2025, KGI, TJL, and the USC Neely Center convened more than 60 experts working on social media and AI chatbot litigation. Participants included staff from state attorneys general offices, private plaintiffs firms, technologists, and technology researchers. Over the course of two days, participants discussed a discussion draft framework[178] for social media and AI chatbot remedies and identified strategies for effective remediation in the technology context.

[177] For information on the universe of cases up to the end of 2025, see Knight-Georgetown Institute et al., "Sources Reviewed."
[178] Knight-Georgetown Institute et al., *Framework for Remedy Discussion Draft*.

Bibliography

Abdo, Alex, Angie Drobnic Holan, Brandon Silverman, et al. *Better Access: Data for the Common Good*. Knight-Georgetown Institute, November 6, 2025. https://kgi.georgetown.edu/research-and-commentary/better-access/.

Abdo, Alex, Ramya Krishnan, Stephanie Krent, Evan Welber Falcón, and Andrew Keane Woods. *A Safe Harbor for Platform Research*. Knight First Amendment Institute at Columbia University, January 19, 2022. https://knightcolumbia.org/content/a-safe-harbor-for-platform-research.

ACLU. "In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law." May 9, 2022. https://live-aclu-wp.pantheonsite.io/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.

Allyn, Bobby. "Jury finds Meta and Google negligent in social media harms trial." *NPR*, March 25, 2026. https://www.npr.org/2026/03/25/nx-s1-5746125/meta-youtube-social-media-trial-verdict.

Anti-Defamation League. *Block/Filter/Notify: Support for Targets of Online Hate Report Card*. Center for Technology and Society, July 31, 2023. https://www.adl.org/resources/report/blockfilternotify-support-targets-online-hate-report-card.

Arnao, Zander, Felix Chen, Alissa Cooper, et al. *Designing the Technical Committee for the United States v. Google Search Antitrust Remedy: A Blueprint for Effective Implementation*. https://kgi.georgetown.edu/wp-content/uploads/2026/04/Designing_the_Technical_Committee_Report_KGI-FINAL-April-2026.pdf.

Atabey, Ayca, Nicholas Dunn, Pedro Hartung, et al. *Children & AI Design Code*. 5Rights Foundation, March 2025. https://5rightsfoundation.com/wp-content/uploads/2025/03/5rights_AI_CODE_DIGITAL.pdf.

Austin, Roy L. "An Update on Our Ads Fairness Efforts." Meta, January 9, 2023. https://about.fb.com/news/2023/01/an-update-on-our-ads-fairness-efforts/.

Bamberger, Kenneth A., and Deirdre K. Mulligan. "Privacy on the Book and on the Ground." *Stanford Law Review* 247 (2011): 247-316. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385.

Bellan, Rebecca. "Father Sues Google, claiming Gemini chatbot drove son into fatal delusion." *TechCrunch*, March 4, 2026. https://techcrunch.com/2026/03/04/father-sues-google-claiming-gemini-chatbot-drove-son-into-fatal-delusion/.

Bogen, Miranda, and Princess Sampson. *It's (Getting) Personal: How Advanced AI Systems Are Personalized*. Center for Democracy & Technology, May 2, 2025. https://cdt.org/insights/its-getting-personal-how-advanced-ai-systems-are-personalized/

Children and Screens, Center for Countering Digital Hate, and ParentsTogether. "Comments to the Office of the New York State Attorney General on the Proposed Rules for the SAFE for Kids Act." December 2025. https://www.childrenandscreens.org/newsroom/news/children-and-screens-submits-expert-comments-on-safe-for-kids-act-proposed-rules/.

Consent Decree Monitor. "The Consent Decree." Accessed May 7, 2026. https://nopdconsent.azurewebsites.net/the-consent-decree.

Cover, Rob, Jennifer Beckett, Benedetta Brevini, Catharine Lumby, Rhyle Simcock, and Jay Daniel Thompson. “Reporting Online Abuse to Platforms: Factors, Interfaces and the Potential for Care.” *Convergence* 32, no. 1 (2026): 142-158. https://doi.org/10.1177/13548565251324508l.

Cunningham, Tom, Sana Pandey, Leif Sigerson, et al. “Ranking by engagement and non-engagement signals: Learnings from industry.” *Annals of the New York Academy of Sciences* 1151 (2025): 19-32. https://nyaspubs.onlinelibrary.wiley.com/doi/10.1111/nyas.15399.

De Freitas, Julian, Zeliha Oguz-Uguralp, and Amhet Kaan-Uguralp. “Emotional Manipulation by AI Companions.” Last modified October 7, 2025. https://arxiv.org/abs/2508.19258.

De Mooy, Michelle. “How to Strengthen the FTC Privacy & Security Consent Decrees.” Center for Democracy and Technology, April 18, 2018. https://cdt.org/insights/how-to-strengthen-the-ftc-privacy-security-consent-decrees/.

Electronic Privacy Information Center. “EPIC’s Model Age-Appropriate Design Code (AADC) Model Legislation.” Accessed May 6, 2026. https://epic.org/epic-model-aadc/.

Engstrom, Nora Freeman, and Robert L. Rabin. “Pursuing Public Health Through Litigation: Lessons from Tobacco and Opioids.” *Stanford Law Review* 73 (2021): 285-362. https://law.stanford.edu/wp-content/uploads/2022/07/Engstrom-Rabin-73-Stan.-L.-Rev.-285-1.pdf.

Faviero, Michelle, Monica Anderson, and Eugenie Park. “Teens, Social Media, and Mental Health.” Pew Research Center, April 22, 2025, https://www.pewresearch.org/internet/2025/04/22/teens-social-media-and-mental-health/.

Federal Trade Commission. *Bringing Dark Patterns to Light*. September 2022. https://www.ftc.gov/reports/bringing-dark-patterns-light.

———. “Data to Go: An FTC Workshop on Data Portability.” September 22, 2020. https://www.ftc.gov/news-events/events/2020/09/data-go-ftc-workshop-data-portability.

———. “Disney to Pay $10 Million to Settle FTC Allegations the Company Enabled the Unlawful Collection of Children’s Personal Data.” September 2, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/09/disney-pay-10-million-settle-ftc-allegations-company-enabled-unlawful-collection-childrens-personal.

———. “FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service.” November 3, 2022. https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service.

———. “Statement of Chairman Joe Simons & Commissioners Noah Joshua Phillips & Christine S. Wilson In re Facebook, Inc.” July 24, 2019. https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf.

Guidehouse. *VRS Compliance Metrics Verification Report*. Meta, March 1, 2024. https://www.justice.gov/crt/media/1345261/dl.

Goland, Joshua A. “Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC’s Newest Enforcement Tool for Bad Data.” *Richmond Journal of Law & Technology* 29, no. 2 (2023). https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1519&context=jolt.

Grout, Kevin. “AG Coleman Sues AI Chatbot Company for Preying on Children.” Kentucky Office of the Attorney General. January 8, 2026. https://www.kentucky.gov/Pages/Activity-stream.aspx?n=AttorneyGeneral&prId=1857.

Hanauer, Peter, John Slade, Deborah E. Barnes, Lisa Bero, and Stanton A. Glantz. “Lawyer Control of Internal Scientific Research to Protect Against Products Liability Lawsuits: The Brown and Williamson Documents.” *JAMA* 274, no. 3 (July 19, 1995): 234–240. https://jamanetwork.com/journals/jama/article-abstract/389239.

Helmore, Edward. “Florida to open criminal investigation into OpenAI over ChatGPT’s influence on alleged mass shooter.” *The Guardian*, April 21, 2026. https://www.theguardian.com/us-news/2026/apr/21/florida-openai-chatgpt-investigation.

Horwitz, Jeff. “Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show.” *Reuters*, November 6, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

Hubbard, Sarah. “Utah Digital Choice Act: Reshaping Social Media.” Harvard Kennedy School Ash Center for Democratic Governance and Innovation, June 10, 2025. https://ash.harvard.edu/resources/utah-digital-choice-act-reshaping-social-media/.

Hurt, Richard D., Jon O. Ebbert, Monique E. Muggli, Nikki J. Lockhart, and Channing R. Robertson. “The Open Doorway to Truth: Legacy of the Minnesota Tobacco Trial.” *Mayo Clinic Proceedings* 84, no. 5 (2009): 446-456. https://www.mayoclinicproceedings.org/article/S0025-6196(11)60563-6/fulltext.

Institute of Electrical and Electronics Engineers. “IEEE Standard for Online Age Verification.” May 24, 2024. https://standards.ieee.org/ieee/2089.1/10700/.

International Organization for Standardization. “ISO/IEC 27566-1:2025 Information security, cybersecurity and privacy protection — Age assurance systems.” December 2025. https://www.iso.org/standard/88143.html.

Jerome, Joseph. “Can FTC Consent Orders Effectively Police Privacy?” *IAPP*, November 27, 2018. https://iapp.org/news/a/can-ftc-consent-orders-police-privacy.

Jones, Meg Leta. *The Character of Consent: The History of Cookies and the Future of Technology Policy*. MIT Press, 2024. https://direct.mit.edu/books/monograph/5797/The-Character-of-ConsentThe-History-of-Cookies-and.

Kang, Cecilia. “Snap Settles Social Media Addiction Lawsuit Ahead of Landmark Trial.” *The New York Times*, January 20, 2026. https://www.nytimes.com/2026/01/20/technology/snap-social-media-addiction-lawsuit.html.

———. “TikTok Settles Social Media Addiction Lawsuit Ahead of a Landmark Trial.” *The New York Times*, January 27, 2026. https://www.nytimes.com/2026/01/27/technology/tiktok-settlement-social-media-addiction-lawsuit.html.

Knight-Georgetown Institute, Tech Justice Law, and USC Marshall Neely Center for Ethical Leadership & Decision Making. *Framework for Remedy: Litigating Platform Design Discussion Draft*. October 31, 2025.

https://kgi.georgetown.edu/wp-content/uploads/2025/11/Framework-for-Remedy-Litigating-Platform-Design-Discussion-Draft.pdf.

———. “Sources Reviewed.” Accessed May 7, 2026. https://drive.google.com/file/d/1Xe7wwTNC-7k0sHZTxzj5sBJ8POWnQRNt/view.

———. “Taxonomy - Mapping Consumer Harm to Specific Social Media Design Elements.” Accessed May 7, 2026. https://docs.google.com/spreadsheets/d/10-ojejxc6a33-1fS0O-prVZgu02_GjNHjm89vNSxQ5s/edit?gid=207813296#gid=207813296.

Kosmyna, Nataliya, Eugene Hauptmann, Ye Tong Yuan, et al. “Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task.” Last modified December 31, 2025. https://www.media.mit.edu/publications/your-brain-on-chatgpt/.

Leerssen, Paddy. "From Murdoch to Musk: Platform Ownership and the Political Economy of Online Content Governance." *Platforms & Society* 2 (2025). https://doi.org/10.1177/29768624251386260.

Legal Information Institute. “monetary relief.” Cornell Law School. Accessed May 6, 2026. https://www.law.cornell.edu/category/keywords/monetary_relief.

———. “settlement.” Cornell Law School. Accessed May 6, 2026. https://www.law.cornell.edu/wex/settlement.

Longpre, Shayne, Sayash Kapoor, Kevin Klyman, et al. "A Safe Harbor for AI Evaluation and Red Teaming." March 7, 2024. https://arxiv.org/abs/2403.04893.

Lubin, Nathaniel, and Ravi Iyer. “How Tech Regulation Can Leverage Product Experimentation Results.” *Lawfare*, July 11, 2023. https://www.lawfaremedia.org/article/how-tech-regulation-can-leverage-product-experimentation-results.

Lubin, Nathaniel, Yuning Liu, Amanda Yarnell, et al. “Social Media Harm Abatement: Mechanisms for Transparent Public Health Assessment.” Annals of the New York Academy of Sciences 1549, no. 1 (2025): 171-184. https://nyaspubs.onlinelibrary.wiley.com/doi/10.1111/nyas.15345.

Martinez, Veronica Root. “Independent Monitorships.” In *Cambridge Handbook on Organizational Culture and Misconduct*. Duke Law School Public Law & Legal Theory Series, 2026 (forthcoming). http://dx.doi.org/10.2139/ssrn.6065806.

Moehring, Alex, Alissa Cooper, Arvind Narayanan, et al. *Better Feeds: Algorithms That Put People First*. Knight-Georgetown Institute, March 2025. https://kgi.georgetown.edu/research-and-commentary/better-feeds/.

Moran, Rachel Elizabeth, Joseph Schafer, Mert Bayar, and Kate Starbird. “The End of Trust and Safety?: Examining the Future of Content Moderation and Upheavals in Professional Online Safety Efforts.” In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, April 25, 2025. https://doi.org/10.1145/3706598.3713662.

National Association of Attorneys General. “Joint Letter to AI Industry Leaders on Child Safety.” August 25, 2025. https://www.naag.org/policy-letter/joint-letter-to-ai-industry-leaders-on-child-safety/.

———. “The Master Settlement Agreement.” Accessed May 6, 2026. https://www.naag.org/our-work/naag-center-for-tobacco-and-public-health/the-master-settlement-agreement/.

Ndubisi, Awele, Felix Agyapong-Opoku, and Belinda Agyapong. “Social Media Use and Sleep Quality in Adolescents and Young Adults: A Scoping Review of Reviews.” *Children* 13, no. 51 (2026). https://pmc.ncbi.nlm.nih.gov/articles/PMC12840076/.

New Mexico Department of Justice. “New Mexico Department of Justice Wins Landmark Verdict Against Meta.” March 24, 2026. https://nmdoj.gov/press-release/new-mexico-department-of-justice-wins-landmark-verdict-against-meta/.

Nguyen, Stephanie T., Erie Meyer, and Samuel A.A. Levine. *AI Companions & Harms to Children*. Georgetown Law Institute for Technology Law & Policy, September 25, 2025. https://www.law.georgetown.edu/tech-institute/research-insights/insights/ai-companions-harms-to-children/.

Nguyen, Stephanie, Erie Meyer, Samuel A.A. Levine, and Patrick Yurky. *Remedies for Tech-Related Harms Chapter 2: Bans on Sharing & Selling Data*. Georgetown Law Institute for Technology Law & Policy, October 29, 2025. https://www.law.georgetown.edu/tech-institute/insights/remedies-for-tech-related-harms-chapter-2/.

Nielsen, Jakob. “How I Developed the 10 Usability Heuristics.” *Jakob Nielsen on UX*, February 15, 2024. https://jakobnielsenphd.substack.com/p/usability-heuristics-history.

Office of the Attorney General for the District of Columbia. “Attorney General Racine Reaches $120 Million Settlement with General Motors Company Over Defective Ignition Switches.” October 19, 2017. https://oag.dc.gov/release/attorney-general-racine-reaches-120-million.

Office of the New York State Attorney General. “Attorney General James Announces $85 Million Multistate Settlement with Honda Over Airbag Failures.” August 25, 2020. https://ag.ny.gov/press-release/2020/attorney-general-james-announces-85-million-multistate-settlement-honda-over.

Open _Future. “_A Public, Interoperable Social Media Space.” Accessed May 6, 2026. https://openfuture.eu/policies-for-the-digital-commons/interoperable-social-media/.

Phang, Jason, Michael Lampe, Lama Ahmad, et al. “Investigating Affective Use and Emotional Well-being on ChatGPT.” April 4, 2025. https://arxiv.org/abs/2504.03888.

Portland Police Bureau Office of the Inspector General. *PPB Force Analysis Annual Summary Report 2025*. Portland Police Bureau, February 2026. https://www.portland.gov/police/doj/documents/force-data-summary-report-2025-annual/download.

Potter, Yujin, Ella Corren, Gonzalo Munilla Garrido, Chris Hoofnagle, and Dawn Song. ”The Gap Between Data Rights Ideals and Reality.” Last modified April 23, 2025. https://arxiv.org/pdf/2312.01511.

Rescorla, Eric, and Alissa Cooper. “First Steps Toward Operationalizing Age Assurance Mandates: New York SAFE for Kids Act Proposed Rules.” Knight-Georgetown Institute, March 12, 2026. https://kgi.georgetown.edu/research-and-commentary/first-steps-toward-operationalizing-age-assurance-mandates-new-york-safe-for-kids-act-proposed-rules/.

Rescorla, Eric, Zander Arnao, and Alissa Cooper. *Age Assurance Online: A Technical Assessment of Current Systems and Their Limitations*. Knight-Georgetown Institute, January 2026.

https://kgi.georgetown.edu/wp-content/uploads/2026/01/Age_Assurance_Online_Technical-Assessment_Report_KGI.pdf.

Responsible Gambling Council. “Looking to take a break from gambling?” Accessed May 6, 2026. https://responsiblegambling.org/for-the-public/problem-gambling-help/self-exclusion/.

Rocha, Natallie. “Google and Character.AI to Settle Lawsuit Over Teenager’s Death.” *The New York Times*, January 7, 2026. https://www.nytimes.com/2026/01/07/technology/google-characterai-teenager-lawsuit.html.

Schermer, Bart W., Bart Custers, and Simone van der Hof. “The crisis of consent: how stronger legal protection may lead to weaker consent in data protection.” *Ethics and Information Technology* 16, no. 2 (2014): 171–182. https://link.springer.com/article/10.1007/s10676-014-9343-8.

Shakhina, Natalia, Pinelopi Skotida, Sujatha Krishnan-Barman, et al. “How Does the Design of Social Media Content Controls Shape Users’ Choice? Evidence from an Online Experiment.” *Behavioural Public Policy* (2025): 1–18. https://doi.org/10.1017/bpp.2025.10016.

Shen, Wen W. *National Opioid Litigation: Settlement Agreements as of January 2025*. Congressional Research Service, February 19, 2025. https://www.congress.gov/crs_external_products/LSB/PDF/LSB11270/LSB11270.6.pdf.

Shiffman, Naomi, and Brandon Silverman. *The Case for Transparency: How Social Media Platform Data Access Leads to Real-World Change*. The George Washington University Institute for Data, Democracy & Politics, May 7, 2025. https://iddp.gwu.edu/sites/g/files/zaxdzs5791/files/2025-05/case_for_transparency_shiffman_silverman.pdf.

Social Media Victims Law Center and Tech Justice Law. “Social Media Victims Law Center and Tech Justice Law Project lawsuits accuse ChatGPT of emotional manipulation, supercharging AI delusions, and acting as a ‘suicide coach’.” November 6, 2025. https://socialmediavictims.org/press-releases/smvlc-tech-justice-law-project-lawsuits-accuse-chatgpt-of-emotional-manipulation-supercharging-ai-delusions-and-acting-as-a-suicide-coach/.

Smutny, Zdenek, and Frantisek Sudzina. “What Affects Work Performance When Using AI Chatbots? Investigating Mediations and Factors Affecting Performance Expectancy and Intentions to Use ChatGPT.” *International Journal of Human-Computer Interaction* (2025): 1-25. https://www.tandfonline.com/doi/full/10.1080/10447318.2025.2573037.

Stoilova, Mariya, Monica Bulger, and Sonia Livingstone. “Do Parental Control Tools Fulfil Family Expectations for Child Protection? A Rapid Evidence Review of the Contexts and Outcomes of Use.” *Journal of Children and Media* 18, no. 1 (2024): 29–49. https://doi.org/10.1080/17482798.2023.2265512.

Tech Justice Law. “Big Win in our Character AI Lawsuit! TJLP Statement on the Motion to Dismiss Decision.” May 21, 2025. https://techjusticelaw.org/updates/big-win-in-our-character-ai-lawsuit-tjlp-statement-on-the-motion-to-dismiss-decision/.

Tech Justice Law, Knight-Georgetown Institute, and Georgetown University Communication, Culture & Technology Program. “Tech Related Actions and Litigation: The TRAL Tracker.” Accessed May 7, 2026. https://techjusticelaw.org/resources/tracker/.

United States. “ACCESS Act.” May 7, 2025. https://www.congress.gov/bill/119th-congress/senate-bill/1634/all-info.

———. “Platform Accountability and Transparency Act.” December 1, 2025. https://www.congress.gov/119/bills/s3292/BILLS-119s3292is.pdf.

United States Department of Justice. "Department of Justice and Montgomery County, Maryland enter into voluntary agreement addressing police practices.” Spring 2000. https://www.justice.gov/crt/federal-coordination-and-compliance-section-163.

———. “Justice Department Reaches Proposed Settlement with Greystar, the Largest U.S. Landlord, to End Its Participation in Algorithmic Pricing Scheme.” August 8, 2025. https://www.justice.gov/opa/pr/justice-department-reaches-proposed-settlement-greystar-largest-us-landlord-end-its.

———. “Justice Department Secures Agreement with Cumberland County Addressing Mental Health Care, Suicide Prevention and Medication-Assisted Treatment for Opiate Withdrawal at the Cumberland County Jail.” May 17, 2023. https://www.justice.gov/archives/opa/pr/justice-department-secures-agreement-cumberland-county-addressing-mental-health-care-suicide.

———. “Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising.” June 21, 2022. https://www.justice.gov/archives/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

———. “New Jersey Settles Allegations of Discrimination by State Police Under Justice Department Agreement.” December 22, 1999. https://www.justice.gov/archive/opa/pr/1999/December/607cr.html.

United States Judicial Panel on Multidistrict Litigation. “Pending MDL Dockets by District.” March 2, 2026. https://www.jpml.uscourts.gov/sites/jpml/files/Pending_MDL_Dockets_By_District-March-2-2026.pdf.

United States Senate Judiciary Subcommittee on Privacy, Technology, and the Law. “Hidden Harms: Examining Whistleblower Allegations that Meta Buried Child Safety Research.” September 9, 2025. S.Hrg. 119-255 — HIDDEN HARMS: EXAMINING WHISTLEBLOWER ALLEGATIONS THAT META BURIED CHILD SAFETY RESEARCH | Congress.gov.

University of California, San Francisco. “About the Truth Tobacco Industry.” Accessed May 6, 2026. https://www.industrydocuments.ucsf.edu/tobacco/.

———. “About OIDA.” Opioid Industry Documents Archive. Accessed March 25, 2026. https://www.industrydocuments.ucsf.edu/opioids/more-resources/about-oida/.

———. “Juul Labs Collection.” JUUL Labs Document Collection. Accessed May 10, 2026. https://www.industrydocuments.ucsf.edu/tobacco/collections/juul-labs-collection/.

USC Marshall Neely Center for Ethical Leadership & Decision Making. “*Neely Center Design Code for Social Media*.” Accessed May 6, 2026. https://docs.google.com/document/d/1RkyeT8m94uHnftuahdctrmn6vF-AeCXUj7YbxB5mU4g/edit?tab=t.0#heading=h.3pgrdj2eu5wd.

Vilk, Viktorya, and Kat Lo. *Shouting into the Void: Why Reporting Abuse to Social Media Platforms Is So Hard and How to Fix It.* PEN America and Meedan, June 29, 2023. https://pen.org/report/shouting-into-the-void/.

Vogels, Emily A. *Teens and Cyberbullying 2022.* Pew Research Center, December 15, 2022. https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

World Health Organization. *The Tobacco Industry Documents: What They Are, What They Tell Us, and How to Search Them — A Practical Manual*. 2004. https://escholarship.org/uc/item/791460pm.

YouTube Privacy Settlement. "Hubbard v. Google." Accessed May 6, 2026. https://youtubeprivacysettlement.com/home/.

Young People's Alliance. "A Bill to Save Human Connection From Human-Like AI Companions." Accessed May 6, 2026. https://docs.google.com/document/d/1TyAHE2AjkEUKcQWV5aWVh7aU6MgdSmJ9Tib5kt5gJFY/edit?usp=sharing.

Zivnuska, Suzanne, John R. Carlson, Dawn S. Carlson, Ranida B. Harris, and Kenneth J. Harris. "Social media addiction and social media reactions." *The Journal of Social Psychology* 159, no. 6 (2019): 746-760. https://www.tandfonline.com/doi/full/10.1080/00224545.2019.1578725.