epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

on

Request for Comment Regarding Youth Mental Health, Safety & Privacy Online

88 Fed. Red. 67,733

November 16, 2023

The Electronic Privacy Information Center (EPIC) submits these comments in response to the National Telecommunications and Information Administration (NTIA)'s Request for Comment (RFC) on the Initiative to Protect Youth Mental Health, Safety & Privacy Online.[1] In conjunction with the United States government's Task Force on Kids Online Health & Safety, the NTIA issued this RFC seeking information about the myriad risks of "health (including mental health), safety, and privacy harms to minors arising from the use of online platforms."[2]

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[3] EPIC regularly advocates for privacy safeguards for minors online.[4] Children and teens online are particularly vulnerable to the effects of commercial surveillance practices like profiling, data misuse, and targeted advertising. The NTIA should focus the Task Force's efforts on the harmful design practices and extensive data collection that perpetuate commercial surveillance of children and teens. To address these issues, the NTIA and Task Force should center data minimization principles in any recommendations or guidance concerning products, services, and platforms used by minors.

Below, we address several of the questions raised in the RFC and provide additional references and resources in a bullet-point list after each response.

---

[1] Initiative to Protect Youth Mental Health, Safety & Privacy Online Request for Comment, 88 Fed. Red. 67,733 (Oct. 2, 2023), https://www.federalregister.gov/documents/2023/10/02/2023-21606/initiative-to-protect-youth-mental-health-safety-and-privacy-online.
[2] *Id.*
[3] EPIC, *About Us* (2023), https://epic.org/about/.
[4] EPIC, *Children's Privacy* (2023), https://epic.org/issues/data-protection/childrens-privacy/.

epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

I. Harms to Minors

5. What are the current and merging risks of harms to minors associated with social media and other online platforms?

c. What harms or risks of harm do social media and other online platforms facilitate with respect to, or impose upon, minors?

d. What are the specific design characteristics that most likely lead to behavior modifications leading to harms or risks?

Children and teens live much of their lives online. From educational settings to toys, gaming, and social media, their online presence is constantly monitored, often without their knowledge or consent. The sweeping collection of personal data from such a young age causes privacy and data security harms to minors in ways that are largely unavoidable. Incomprehensible privacy disclosures, deceptive design elements, broad commercial surveillance practices, and targeted advertising make the digital ecosystem too complex for adults—let alone minors—to fully understand. Existing laws like the Children's Online Privacy and Protection Act (COPPA) do not sufficiently protect minors from the myriad harmful effects of commercial surveillance systems.[5]

Minors are uniquely vulnerable to the effects of these commercial surveillance systems. The constant monitoring and profiling of children online can make it difficult to develop a sense of autonomy and personality.[6] Design tools fueled by sophisticated profiling use nudging techniques and manipulative patterns to alter or predetermine the universe of options and choices available. In the targeted advertising context, sellers have tremendous power, taking advantage of this informational asymmetry and the still-developing critical thinking skills of children and teens to target young people for commercial gain.[7]

Risks of harms to minors online also stem from design characteristics, like engagement-optimizing algorithms. In whistleblower Frances Haugen's testimony to Congress, Haugen described how design decisions contribute to commercial surveillance systems: "Facebook was collecting data points on every click, every piece of content viewed, and ever search query to build profiles about teenagers in order to keep them online for longer, to keep the commercial

---

[5] Comments of EPIC in re the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security, 177 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM- comments-Nov2022.pdf [hereinafter EPIC FTC Comments on Commercial Surveillance].

[6] *See* Elizabeth Laird et al., *Hidden Harms: The Misleading Promise of Monitoring Students Online*, Center for Democracy and Technology (Aug. 3, 2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/.

[7] Dylan Williams et al., Reset Australia, *Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data* 22 (2021), https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf.

surveillance cycle going, and to optimize Facebook's profits."[8] Recently, 41 states sued Meta on the grounds that these design features are addictive, often leading to other mental health harms.[9] In addition to psychological harms, children and teens face risks to physical safety like self-harm, stalking, bullying, and unwanted messaging or attention from adults.[10] Some of these harms are exacerbated with the increased, unfettered access and use of artificial intelligence. For example, young women and girls have increasingly been the targets of a surge of AI-generated fake nude images, causing extreme emotional distress and reputational damage.[11]

- EPIC's Comments in re the FTC's ANPR on Commercial Surveillance & Data Security: *Disruption Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*[12]
  - The Privacy of Minors (p. 167)
- *Holding Big Tech Accountable: Legislation to Build a Safer Internet: Hearing before the Subcomm. Consumer Protect. of the H. Comm. on Energy & Com.*, 117th Cong. (2021) (testimony of Josh Golin, Exec. Dir., Fairplay)[13]
- Dylan Williams et al., Reset Australia, *Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data* 22 (2021)[14]
- Frances Haugen, Statement of Frances Haugen, *United States Senate Committee on Commerce, Science, and Transportation, Sub-Committee on Consumer Protection, Product Safety, and Data Security* (Oct. 4, 2021)[15]
- Nico Grant et al., *YouTube Ads May Have Led to Online Tracking of Children, Research Says*, N.Y. Times (Aug. 17, 2023)[16]
- Jeff Horwitz, *His Job Was to Make Instagram Safe for Teens. His 14-Year-Old Showed Him What the App Was Really Like*, Wall Street Journal (Nov. 2, 2023)[17]

---

[8] EPIC FTC Comments on Commercial Surveillance at 171 (summarizing Frances Haugen's testimony).
[9] Christiano Lima & Naomi Nix, *41 States Sue Meta, Claiming Instagram, Facebook are Addictive, Harm Kids*, Washington Post (Oct. 23, 2023), https://www.washingtonpost.com/technology/2023/10/24/meta-lawsuit-facebook-instagram-children-mental-health/.
[10] Jeff Horwitz, *His Job Was to Make Instagram Safe for Teens. His 14-Year-Old Showed Him What the App Was Really Like*, Wall Street Journal (Nov. 2, 2023), https://www.wsj.com/tech/instagram-facebook-teens-harassment-safety-5d991be1.
[11] Pranshu Verma, *AI fake nudes are booming. It's ruining real teen's lives*, Washington Post (Nov. 5, 2023), https://www.washingtonpost.com/technology/2023/11/05/ai-deepfake-porn-teens-women-impact/.
[12] https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.
[13] https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/documents/Witness%20Testimony_Golin_CPC_2021.12.09.pdf
[14] https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf.
[15] https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49.
[16] https://www.nytimes.com/2023/08/17/technology/youtube-google-children-privacy.html.
[17] https://www.wsj.com/tech/instagram-facebook-teens-harassment-safety-5d991be1.

- Pranshu Verma, *AI fake nudes are booming. It's ruining real teen's lives*, Washington Post (Nov. 5, 2023)[18]
- Christiano Lima & Naomi Nix, *41 States Sue Meta, Claiming Instagram, Facebook are Addictive, Harm Kids*, Washington Post (Oct. 23, 2023)[19]
- Elizabeth Laird et al., *Hidden Harms: The Misleading Promise of Monitoring Students Online*, Center for Democracy and Technology (Aug. 3, 2022)[20]

II. Market Conditions and Structure

2. Are there particular market conditions or incentives built into the market structure that enhance or deter benefits and/or harms that should be addressed and/or encouraged?

The market conditions of the digital ecosystem incentivize the extraction and sharing of personal information, causing extensive harm to minors in particular. A market characterized by minimal regulation and oversight has allowed for the overcollection and out-of-context use of children's personal information at industrial scale. After decades of rapid growth across the tech sector fueled by the misuse of personal data and attention-maximizing algorithms, market conditions must change to deter the harms that children now face. "[A]gencies are recognizing that the ability to control, collect and use data contributes to a firm's market power. Data provides market actors with knowledge about their customers, users and competitors. This knowledge can lead to unfair and exclusionary market practices."[21] Current market conditions invite companies to hoard and exploit personal data to enrich themselves, often at the expense of minors. For example, Facebook executives ignored internal research that showed teenagers experiencing depression, citing concerns over losing some of the company's $100 billion in ad revenue or youth engagement on the platform.[22]

The best policy tool to change these market dynamics and reduce the resulting harms to minors is a robust data minimization framework: a legal requirement for companies to limit the collection, use, disclosure, and retention of personal information to that which is strictly necessary for the purpose for which it was collected. Establishing such a requirement will undercut the pressure for companies to "keep up" with lucrative but harmful data practices that other firms engage in, which in turn will advance the wellbeing and privacy of minors. The final

---

[18] https://www.washingtonpost.com/technology/2023/11/05/ai-deepfake-porn-teens-women-impact/.
[19] https://www.washingtonpost.com/technology/2023/10/24/meta-lawsuit-facebook-instagram-children-mental-health/.
[20] https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/.
[21] Elettra Bietti, *Data, Context and Competition Policy*, UChicago Booth Stigler Center: Promarket (Mar. 13, 2023), https://www.promarket.org/2023/03/31/data-context-and-competition-policy/.
[22] Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, *Facebook Knows Instagram is Toxic for Teen Girls, Company Documents Show*, Wall Street Journal (Sept. 14, 2021), https://www.wsj.com/articles/facebookknows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

section of these comments offers guidance and policy recommendations to this end. Here, EPIC suggests some resources concerning market conditions that perpetuate harms to children and needed structural changes to prevent those harms.

- EPIC's Comments in re the FTC's ANPR on Commercial Surveillance & Data Security: *Disruption Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*[23]
  - The Privacy of Minors (p. 167)
- EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*[24]
  - p. 20
- Accountable Tech, Petition to Ban Surveillance Advertising[25]
  - "Exploiting Kids and Teens" pp. 32-33
- EPIC's Comments to the DOJ and FTC on Draft Merger Guidelines[26]

III. Current Industry Practices and Emerging Issues Including AI

1. *(h) Do specific applications of artificial intelligence and/or other emerging technologies exacerbate or help alleviate certain harms or risks of harm in this area? If so, which and how?*

Machine learning algorithms are regularly trained on (or facilitate access to) datasets that include the personal information of minors, sometimes in violation of COPPA. Many systems like Clearview AI[27] and ChatGPT[28] are built by scraping information from the public internet. Developers of these tools use web crawlers to index billions of webpages and compile them into datasets for training algorithms. Yet there is often no filter to prevent the personal information of minors from being included in these datasets. Facial recognition tools like Clearview AI and

[23] https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.
[24] https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[25] https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf.
[26] https://epic.org/documents/comments-of-epic-on-ftc-and-doj-draft-merger-guidelines/
[27] Kashmir Hill, *The Secretive Company That Might end Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[28] Dennis Layton, *ChatGPT-Show me the Data Sources*, Medium (Jan. 30, 2023), https://medium.com/@dlaytonj2/chatgpt-show-me-the-data-sources-11e9433d57e8.

PimEyes include photos of children in their databases, including those under age 13.[29] Clearview AI often boasts about its robust dataset, now totaling over 30 billion facial vectors.[30]

Amazon's Alexa, in particular, has caught the FTC's attention for recording children's voice prompts and using that data to train the Alexa algorithm.[31] According to the FTC's complaint against Amazon, the company retained personal information "longer than is reasonably necessary to fulfill the purposes for which the information is collected," did not honor parental data deletion requests in a timely manner, and did not request verifiable parental consent to record the children's voice in violation of COPPA.[32]

In addition to its discriminatory impacts, facial recognition technology poses special risks to children. Until just last month, a person could input an image of a child into facial recognition tool PimEyes to find other pictures of the child posted across the internet.[33] (PimEyes now claims to have blocked searches of children's faces,[34] but how effective that barrier is has yet to be determined.) In theory, PimEyes users are only supposed to use the search engine on their own faces or the faces of those who have consented, but PimEyes does not have any meaningful controls in place to prevent users from searching a non-consenting person's face.[35] Both PimEyes and Clearview AI not only return other pictures of the person identified, but also link to where those images were found.[36] This feature can be used by bad actors to stalk children or find a child's name and address.[37] Below are some additional resources about problems caused by the widespread use of facial recognition systems.

- U.S. Gov't Accountability Off., *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial* Uses 6 (Jul. 2020)[38]
- *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, Nat'l Inst. of Standards and Tech. (Dec. 19, 2019)[39]

---

[29] Kashmir Hill, *Can You Hide a Child's Face From A.I.?*, New York Times (Oct. 14, 2023), https://www.nytimes.com/2023/10/14/technology/artifical-intelligence-children-privacy-internet.html.
[30] Terence Liu, *How We Store and Search 30 Billion Faces*, Clearview AI Blog (Apr. 18, 2023), https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces.
[31] Complaint, *U.S. v. Amazon.com et al.*, W.D. Wa., Case 2:23-cv-00811 (May 31, 2023).
[32] *Id.*
[33] *About PimEyes*, PimEyes, https://pimeyes.com/en/about (last visited Nov. 14, 2023).
[34] Kashmir Hill, *Face Search Engine PimEyes Blocks Searches of Children's* Faces, New York Times (Oct. 23, 2023), https://www.nytimes.com/2023/10/23/technology/pimeyes-blocks-searches-childrens-faces.html.
[35] *Supra* note 25.
[36] *Supra* note 29; *Law Enforcement*, Clearview AI Solutions, https://www.clearview.ai/law-enforcement (last visited Nov. 14, 2023).
[37] *Supra* note 25.
[38] https://www.gao.gov/products/gao-20-522.
[39] https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

- Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News (Feb. 11, 2018)[40]
- Erik Learned-Miller et al., *Facial Recognition Technologies in the Wild: A Call for Federal Office*, Algorithmic Justice League 7 (May 29, 2020)[41]
- Mitchell Clark, *Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can't See Them*, Verge (Apr. 8, 2021)[42]

Generative AI also poses special risks to children. For example, deepfake technology uses real photographs, video recordings, and audio recordings of a person to generate novel photos, videos, and/or audio recordings of the person.[43] In September, attorneys general from all 50 states sent a letter to Congress regarding the use of deepfakes targeting children, particularly in the context of child sexual abuse material (CSAM).[44] Phone scammers are also using deepfakes to mimic children's voices in phone calls to parents to demand ransom money for the "kidnapped" child.[45]

Even setting aside the harmful applications of these tools, the mere collection and processing of a child's facial geometry can itself be harmful. Biometric identifiers are immutable. A person cannot reset their irises or face the same way they can reset a password. At the same time, data breaches are becoming endemic to large data systems.[46] Last month, 23andMe—a popular genetic testing company that collects DNA samples from customers—was hacked,[47] and millions of user records were posted to a cybercrime forum by the hacker.[48] When biometrics are collected from children earlier and earlier in their lives, there is a greater chance

---

[40] https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.
[41] https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf.
[42] https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning.
[43] Adam Satariano & Paul Mozur, *The People Onscreen Are Fake. The Disinformation Is Real.*, New York Times (Feb. 7, 2023), https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html.
[44] National Association of Attorneys General, *54 Attorneys General Call on Congress to Study AI and Its Harmful Effects on Children*, NAAG Press Release (Sep. 5, 2023), https://www.naag.org/press-releases/54-attorneys-general-call-on-congress-to-study-ai-and-its-harmful-effects-on-children/.
[45] *Phone scammers are using artificial intelligence to mimic voices*, CBS Evening News (Jul. 12, 2023), https://www.cbsnews.com/news/artificial-intelligence-phone-scam-fake-voice/.
[46] Kevin Knight, *Why Data Breaches Are Increasing And What CISOs Can Do About It,* Forbes (Apr. 20, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/04/20/why-data-breaches-are-increasing-and-what-cisos-can-do-about-it/?sh=1dcd5e71547e.
[47] Lily Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews,* Wired (Oct. 6, 2023), https://www.wired.com/story/23andme-credential-stuffing-data-stolen/.
[48] Lorenzo Franceschi-Bicchierai, *Hacker leaks millions more 23andMe user records on cybercrime forum,* TechCrunch (Oct. 18, 2023), https://techcrunch.com/2023/10/18/hacker-leaks-millions-more-23andme-user-records-on-cybercrime-forum/.

that a data breach will expose their personal information. Below are resources on the harms stemming from generative AI and the sensitivity of biometric identifiers.

- *Generating Harms: Generative AI's Impact & Paths Forward,* EPIC (May 2023)[49]
- *Comments to the UK ICO's Office for the Consultation on the Draft Biometric Data Guidance,* EPIC (Oct. 20, 2023)[50]
- *Written Testimony in support of Maryland SB169: Biometric Identifiers*, EPIC (Feb. 7, 2023)[51]
- Woodrow Hartzog, *Facial Recognition Is the perfect Tool for Oppression*, Medium (Aug. 2, 2018)[52]

In educational settings, untested and error-prone automated decision-making systems like remote exam proctoring tools can distort student behavior and lead to adverse educational impacts. These systems record video of the student as the student takes an exam, monitoring behaviors like whether the student is looking to the side and whether the student is talking to purportedly identify instances of cheating. Many of these programs have been contested due to their discriminatory nature,[53] and at least one court has ruled that an exam proctoring tool violated the a student's Fourth Amendment rights because it required the student to scan their room with the camera before beginning an exam.[54] Students are facing serious consequences, such as suspension or even expulsion for accusations based on anti-cheating software that prove false. For further resources on the failures of emotional recognition:

- James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game*, The Verge (Apr. 6, 2021)[55]
- Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, The Atlantic (Apr. 27, 2021)[56]
- Charlotte Gifford, *The Problem with Emotion-Detection Technology*, The New Economy (Jun. 15, 2020)[57]

---

[49] https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf.
[50] https://epic.org/documents/epic-comments-to-the-uk-icos-office-for-the-consultation-on-the-draft-biometric-data-guidance/.
[51] https://epic.org/documents/maryland-sb169-biometric-identifiers/.
[52] https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.
[53] Kristy P. Kennedy, *Remote Proctoring Services Are Facing Legal, Legislative Challenges*, Teen Vogue (Oct. 20, 2023), https://www.teenvogue.com/story/remote-proctoring-services-lawsuits.
[54] Amanda Holpuch and April Rubin, *Remote Scan of Student's Room Before Test Violated His Privacy, Judge Rules,* N.Y. Times (Aug. 25, 2022), https://www.nytimes.com/2022/08/25/us/remote-testing-student-home-scan-privacy.html.
[55] https://www.theverge.com/2021/4/6/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game.
[56] https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/.
[57] https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology.

- Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, The Conversation (Jan. 3, 2019)[58]
- _Kashmir Hill, *Microsoft Plans to Eliminate Face Analysis Tools in Push for 'Responsible AI,'* N.Y. Times (Jun. 21, 2022)[59]
- Kate Crawford, *Time to Regulate AI That Interprets Human Emotions*, Nature (Apr. 6, 2021)[60]

For further resources on educational technology and other automated decision-making technologies affecting students, see:

- *Comment on the Department of Education regarding Potential New Program, from Seedlings to Scale*, EPIC (Nov. 13, 2023)[61]
- Complaint, *In re: Online test Proctoring Companies*, EPIC (Dec. 9, 2020)[62]
- *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, EPIC (Nov. 2022), 70-71, 76[63]

Minors are uniquely vulnerable to commercial surveillance, which is necessarily intended to suggest and shape preferences and beliefs. Children and teens are a class of consumers with unique vulnerabilities, but they also engage in a variety of activities on the internet that expose them to the same types of harms of commercial surveillance as an adult would face using the internet. Firstly, there is an informational asymmetry: minors are far less likely to comprehend that something is an advertisement. Research shows only 25% of children between the ages of 8 and 15 were able to distinguish top results from a Google search as advertisements, despite the search results being labeled with the term "ad."[64]

Second, minors are more likely to unknowingly or unwillingly "consent" to expansive data collection or surveillance regimes (to the extent that a minor is in a position to consent to such systems at all).[65] One recent study found that by the time a child turns 13, over 72 million

[58] https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.
[59] https://www.nytimes.com/2022/06/21/technology/microsoft-facial-recognition.html.
[60] https://www.nature.com/articles/d41586-021-00868-5.
[61] https://epic.org/documents/comments-of-epic-to-the-department-of-education-on-seedlings-to-scale/.
[62] https://epic.org/documents/in-re-online-test-proctoring-companies/.
[63] https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.
[64] Ofcom, *Children and Parents: Media Use and Attitudes Report* 12–13 (2017), https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf.
[65] *See e,g,* Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. Univ. L. Rev. 1461 (2019).

data points have been collected about them, excluding trackers used by Facebook, Twitter, YouTube, and other embedded social media widgets.[66]

Finally, schools are increasingly using technology that children are unable to reasonably opt out of. Schools are leasing devices like laptops and tablets to children to use throughout the school year;[67] using exam proctoring software; using learning management systems like Canvas or Blackboard that host student assignments, grades, files, and activities;[68] using emotional recognition surveillance technology to attempt to prevent mass shootings;[69] and buying AI lesson planning technology that can profile and target a child's development,[70] among many others. Researchers at Human Rights Watch analyzed 164 edtech products endorsed in 49 countries during the pandemic, 89% of which were found to have "put at risk or directly violated children's privacy and other children's rights, for purposes unrelated to their education."[71]

6. What practices and technologies do social media and other online platform providers employ today that exert a significant positive or negative effect on minors' health, safety, and privacy?

c. Have the practices of social media and other online platforms evolved over time to enhance or undercut minors' health and safety, including their privacy, in ways that should be taken into account for future efforts? If so, how? For example, what factors have been significant in shaping any such

---

[66] Geoffrey A. Fowler, *Your Kids' Apps Are Spying On Them*, Wash. Post (June 9, 2022), https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy/; see also SuperAwesome, *How Much Data Do Adtech Companies Collect On Kids Before They Turn 13?* (Dec. 13, 2017), https://web.archive.org/web/20180309203314/https://blog.superawesome.tv/2017/12/13/how-much-data-do-adtech-companies-collect-on-kids-before-they-turn-13/.

[67] Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students*, Slate (Feb. 24, 2022), https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html.

[68] Jason Kelley, *Canvas and other Online Learning Platforms Aren't Perfect—Just Ask Students,* Electronic Frontier Foundation (Apr. 27, 2022) https://www.eff.org/deeplinks/2022/04/canvas-and-other-online-learning-platforms-arent-perfect-just-ask-students.

[69] Todd Feathers, *Schools Spy on Kids to Prevent Shootings, But There's No Evidence It Works*, Vice (Dec. 4, 2019) https://www.vice.com/en/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works.

[70] Khari Johnson, *Teachers Are Going All In on Generative AI,* Wired (Sep. 15, 2023), https://www.wired.com/story/teachers-are-going-all-in-on-generative-ai/ ; Nicole Warren-Lee and Lyndsay Grant, *UK announces AI funding for teachers: how this technology could change the profession*, The Conversation (Nov. 9, 2023), https://theconversation.com/uk-announces-ai-funding-for-teachers-how-this-technology-could-change-the-profession-217149.

[71] Hye Jung Han, Human Rights Watch, *"How Dare They Peep into My Private Life?" Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic* (2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.

evolution that are likely to have similar bearing on the future of industry practices?

Family vlogging is a new and evolving genre of social media content that can have a serious negative impact on the children it features. Family vlogging is a genre of content, typically found in the form of regularly posted YouTube videos, that chronicles the daily life of a family. Shortform examples of the genre can also be found on Instagram Reels, YouTube Shorts, and TikTok. These channels can rack up tens of millions of followers and billions of views,[72] and commonly feature children under the age of 10.[73] Family vlogs are also some of the most lucrative types of content because of their family-friendly nature, which can fetch higher advertising rates.[74] But being forced to appear in this content can be invasive and harmful to children.[75] And as noted above, generative AI systems and stalkerware can also exploit images of the children from these publicly posted videos to create deepfakes and disturbingly detailed profiles.

Children are simply not in a position to compel their parents to take down content from the internet. Children have little autonomy to say "no" when they are infants or toddlers, and even as they grow older, it is difficult comprehend the sheer scale of social media and the wide reach a family vlogging video can achieve. The child would not be giving actual informed consent, and what content to post is up to the parents' discretion. Since parents are the ones who run the YouTube channel, children are often also not in the position to delete any content they don't want to be public themselves.[76] Furthermore, children may feel pressured to consent to filming when a family's livelihood depends on their YouTube Channel.[77] Children are essential to the draw of many family vlog channels, so asking a parent to stop posting videos featuring them could feel like the child is asking the parent to stop earning money.

---

[72] *See, e.g.*, The Ace Family, SocialBlade, https://socialblade.com/youtube/channel/UCWwWOFsW68TqXE-HZLC3WIA (last visited Nov. 14, 2023).
[73] *See, e.g.*, The Ace Family, https://www.youtube.com/c/THEACEFAMILY (Last visited Nov. 14, 2023).
[74] Jesselyn Cook, *A Senate Bill Targets YouTube Pedophiles. Could It Cost Family Vloggers Their Livelihood?*, Huffington Post (Jun. 18, 2019), https://www.huffpost.com/entry/senate-bill-pedophiles-youtube-family-vloggers_n_5d0930e0e4b0e560b70a4f1e.
[75] Taylor Lorenz, *There are almost no legal protections for the internet's child stars*, Washington Post (Sept. 1, 2023), https://www.washingtonpost.com/technology/2023/04/08/child-influencers-protections-congress/.
[76] Allie Volpe, *How Parents of Child Influencers Package Their Kids' Lives for Instagram*, The Atlantic (Feb. 28, 2019), https://www.theatlantic.com/family/archive/2019/02/inside-lives- child-instagram-influencers/583675/.
[77] Tiffany Ferg, *The Dark Side of Family Vlogging*, Youtube (Nov. 21, 2018), https://www.youtube.com/watch?v=-yf8 (last visited Nov. 14, 2023).

In the United States, only Illinois has passed a law that would regulate child influencers. The Illinois law mirrors the Coogan Act[78] and merely entitles child influencers to a percentage of earnings.[79] While this is an important first step, it does not include protections to allow children to stay off the internet or remove previous content.[80] A previous version of the bill included a provision enabling former child influencers to request platforms to take down monetized content posted of them as a minor, but the provision did not make it to the final text of the law.[81] Internationally, France passed a law protecting child influencers by creating a right to be forgotten, as well as several child labor protections similar to child actor laws.[82]

The actual substance of family vlogging videos can also be harmful to children, particularly when YouTube's algorithm boosts engagement on videos that garner stronger reactions. YouTube Community Guidelines prohibit the harming of minors and illegal content,[83] as well as "dangerous challenges and pranks,"[84] but the platform's content moderation is spotty at best.[85] A common trope of family vlogging content is prank content, wherein parents play practical jokes on children and film their (often distressed) reactions. In one such instance, a couple lost custody of their child over a prank video posted to YouTube because of the severe emotional distress caused to the child.[86] Family vlogs can often feature intimate and embarrassing moments in a child's life, such as a doctor's visit filled with tears,[87] a child's first

---

[78] Cal. Fam. Code § 6750 et seq.; *See also* Coogan Law, SAG-AFTRA, https://www.sagaftra.org/membership-benefits/young-performers/coogan-law (last visited Nov. 14, 2023).
[79] Angela Yang, *Illinois passed a law to protect child influencers. Advocates are cautiously optimistic more states will follow.*, NBC News (Aug. 15, 2023), https://www.nbcnews.com/news/child-influencers-law-illinois-reaction-rcna99831.
[80] S.B. 1782, 103rd Gen. Assemb. Reg. Sess. (Il. 2023).
[81] *Supra* note 61.
[82] *France passes new law to protect child influencers,* BBC (Oct. 7, 2020), https://www.bbc.com/news/world-europe-54447491.
[83] *Child safety policy*, Youtube, https://support.google.com/youtube/answer/2801999 (last visited Nov. 14, 2023).
[84] Camilla (TeamYoutube), *Announcement: Strengthening enforcement of our Community Guidelines*, Youtube Help (Jan. 15, 2019), https://support.google.com/youtube/thread/1063296?hl=en.
[85] Abby Ohlheiser, *A week later, YouTube condemns a Logan Paul vlog of a suicide victim's body, says it's looking at 'further consequences'*, Wash. Post (Jan. 9. 2018), https://www.washingtonpost.com/news/the-intersect/wp/2018/01/09/a-week-later-youtube-condemns-a-logan-paul-vlog-of-a-suicide-victims-body-says-its-looking-at-further-consequences/.
[86] *DaddyOFive parents lose custody 'over YouTube pranks',* BBC (May 2, 2017), https://www.bbc.com/news/technology-39783670.
[87] The ACE Family, *WE DID NOT WANT TO DO THIS!*, (Apr. 25, 2020), https://www.youtube.com/watch?v=siQITupIIvk.

time shaving,[88] and discussions of a school crush against the child's will.[89] Though popular, the posting of this content without a right to have content removed by the child in question is analogous to the tort of publication of private facts—and can lead to serious harm.[90] A child influencer who testified in a hearing for the Illinois bill stated that she was ostracized and bullied at school due to the content posted by her parents, including videos about her first period and other private medical information.[91] Another child influencer testified that the scripted content she and her siblings were forced to read for the camera, including fake emotional reactions, was upsetting to her at the time.[92] She has been bullied by her peers at school, and even stalked because of her online image.[93]

IV. Identifying Proposed Guidance and/or Policies

11. Are there potential best practices (for example, practices related to design, testing, or configuration) or policies that are not currently employed by social media and other online platforms that should be considered?

16. What guidance, if any, should the United States government issue to advance minors' health, safety, and/or privacy online?

17. What policy actions could be taken, whether by the U.S. Congress, federal agencies, enforcement authorities, or other actors, to advance minors' online health, safety, and/or privacy? What specific regulatory areas of focus would advance protections?

To ensure the health and safety of kids and teens online, any guidance or recommendations from NTIA and the Task Force should shift the burden for risk assessment and avoiding harms from consumers and children to online platforms. Parents and minors do not have a meaningful choice about how personal data is collected and used, and it is nearly impossible to anticipate or avoid online harms. COPPA is a floor, not a ceiling, and Congress should act to pass a comprehensive privacy law like the American Data Privacy and Protection

---

[88] Danya Hajjaji, *YouTube Lets Parents Exploit Their Kids For Clicks*, Newsweek (Oct. 21 2021), https://www.newsweek.com/youtube-lets-lawless-lucrative-sharenting-industry-put-kids-mercy- internet-1635112.

[89] Amanda G. Riggio, *The Small-er Screen: YouTube Vlogging and the Unequipped Child Entertainment Labor Laws*, 44 Seattle Univ. L. Rev. 493, 494 (2021).

[90] Aphrodite Stamboulos, *Family Channels: Violators of Child Privacy*, Fordham Undergraduate L. Rev. Blog, https://undergradlawreview.blog.fordham.edu/digital-privacy/family-channels-violators-of-child-privacy/#easy-footnote-bottom-1-2279.

[91] Katie Collins, *The US Is Finally Dealing With the Exploitation of Child Influencers*, CNET (Feb. 17, 2023), https://www.cnet.com/news/politics/the-us-is-finally-dealing-with-the-exploitation-of-child-influencers/.

[92] Taylor Lorenz, *There are almost no legal protections for the internet's child stars*, Washington Post (Sept. 1, 2023), https://www.washingtonpost.com/technology/2023/04/08/child-influencers-protections-congress/.

[93] *Id.*

Act (ADPPA) that includes provisions to protect kids online.[94] The ADPPA, or any other regulatory or legislative action to address these issues, should center data minimization principles. For example, EPIC has advocated for the Federal Trade Commission to consider it an unfair trade practice to "collect, process, retain or transfer the personal data of minors under the age of 18 unless strictly necessary to achieve the minor's specific purpose for interacting with the business or to achieve certain essential purposes."[95]

Fueled by excessive data collection, the harmful design practices that enable the cycle of commercial surveillance are another focus area for regulation, legislation, or guidance. Platforms and products are typically designed with profit in mind rather than the wellbeing of children and teens. To maximize engagement and increase revenue, many companies make design choices that facilitate data collection but put children and teens at risk.[96] Banning targeted advertising directed at minors and regulating how companies monetize minors' data would force companies to change their business practices without restricting online access for children and teens.

- EPIC's Comments for FTC's ANPR on Commercial Surveillance & Data Security: *Disruption Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*[97]
  - The Privacy of Minors (p. 167)
- 5Rights Foundation, *Pathways: How Digital Design Puts Children at Risk* 7 (2021).[98]
- Center for Digital Democracy et al., *Petition for FTC Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement*, (Nov. 17, 2022).[99]

V. Conclusion

EPIC applauds the NTIA's attention to the important issues shaping privacy, security, and safety for minors online. EPIC is eager to engage with the NTIA further on the issues raised in this comment, including the harms minors face online, the market conditions that fuel commercial surveillance and pose unique risks to minors online, emerging risks from AI and other technologies, and implementing safeguards like data minimization and a ban on targeted advertising to minors.

---

[94] House Energy and Commerce Committee, *Protecting Kids' Privacy with a National Data Privacy and Security Standard*, (May 8, 2023), https://energycommerce.house.gov/posts/protecting-kids-privacy-with-a-national-data-privacy-and-security-standard.
[95] EPIC FTC Comments on Commercial Surveillance at 167.
[96] 5Rights Foundation, *Pathways: How Digital Design Puts Children at Risk* 7 (2021), https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf.
[97] https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.
[98] https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf.
[99] https://fairplayforkids.org/wp-content/uploads/2022/11/EngagementPetition.pdf.

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Respectfully submitted,

/s/ John Davisson
John Davisson
EPIC Director of Litigation

/s/ *Sara Geoghegan*
Sara Geoghegan
EPIC Counsel

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Law Fellow

/s/ *Maria Villegas Bravo*
Maria Villegas Bravo
EPIC Law Fellow