DAY ONE PROJECT

Protecting Children's Privacy at Home, at School, and Everywhere in Between

Ariel Fox Johnson

December 2020

Summary

Young people today face surveillance unlike any previous generation, at home, at school, and everywhere in between. Constant use of technology while their brains are still developing makes them uniquely vulnerable to privacy harms, including identity theft, cyberbullying, physical risks, algorithmic labeling, and hyper-commercialism. A lack of privacy can ultimately lead children to self-censor and can limit their opportunities. Already-vulnerable populations—who have fewer resources, less digital literacy, or are non-native English speakers—are most at risk.

Congress and the Federal Trade Commission (FTC) have repeatedly considered efforts to better protect children's privacy, but the next administration must ensure that this is a priority that is actually acted upon by supporting strong privacy laws and providing additional resources and authority to the FTC and support to the Department of Education (ED). The next administration should also establish a task force to explore how to best support and protect students. And the FTC should use its current authority to increase its understanding of the children's technology market and robustly enforce a strong Children's Online Privacy Protection Act (COPPA) rule.

Challenge and Opportunity

Young people live in an always-on culture where they are constantly connected—and required to be to get an education—and where powerful tech interests take advantage of young people's hardwired instinct to share. They are early adopters of new and often inexpensive technology, with safety and privacy features that are often an afterthought. The privacy of all individuals is an urgent challenge that must be addressed, and that the next administration and Congress should prioritize. Furthermore, policymakers must explicitly consider the unique vulnerabilities of children and teenagers. The United States is long overdue to increase privacy protections for children, and to add them for teenagers, who are presently ignored under federal law. The U.S. is increasingly falling behind in its protections,[1] and it is critical that policymakers protect privacy at home, at school, and everywhere in between.

Young People are Spending More Time Online and are Uniquely Vulnerable

Children and teenagers are spending more time online and on connected devices. Kids under age 8 spent an average of 38 minutes a day on mobile devices in 2017, up from 15 minutes a day in 2013.[2] In 2019, a majority of 11-year-olds owned smartphones; compared with less than a third in 2015. In 2019, more than twice as many tweens and teens watched online videos every day than in 2015, and the average time spent watching videos roughly doubled. Furthermore, even before the pandemic, young people were increasingly required to use technology for

[1] See, e.g., the EU's General Data Protection Regulation (GDPR); Brazil's General Data Protection Law (LGPD); UK's Age-Appropriate Design Code.

[2] Rideout, Victoria. 2017. The Common Sense Census: Media use by kids age zero to eight. Common Sense Media, San Francisco, CA.

school. In 2019, tweens and teens were twice as likely to use computers every day for homework than they were in 2015.[3]

Young people are emotionally and cognitively different than adults in ways that exacerbate the risks of their extensive time online. Children and teenagers lag behind adults in conceptualizing privacy, making sense of online data flows, understanding terms of service, and recognizing advertisements.[4] Young people's developing brains, which have trouble comprehending the persuasive intent of advertisements and understanding long-term consequences, let alone complicated data ecosystems, are no match for advanced profiling and analytics techniques. Both young children and teenagers are prone to overshare; the former are unable to understand the meaning of their actions while the latter are more likely to engage in risky behavior.[5] This leaves children and teenagers at risk from hyper-commercialism, physical safety concerns, heightened emotional and behavioral harms, cyberbullying, identity theft, manipulation, and algorithmic labeling and limiting that can impact their current and future opportunities. Indeed, heavy social media usage in youth has been associated in some studies with an elevated chance of suicidal ideation, a leading cause of death among older children and teenagers today.[6] Risks appear to be greater for individuals in families with lower levels of education, with some studies showing that children of parents without college degrees are at higher risk for privacy violations.[7] Furthermore, awareness of surveillance and privacy exposure can lead young people to self-censor or to limit their attempts to engage with or understand the world. Technology can "surveil, sort and steer people on a massive scale"[8]; it can also suppress speech and behavior, especially from young people.

---

[3] Rideout, Victoria and Michael Robb. 2019. The Common Sense census: Media use by tweens and teens. Common Sense Media, San Francisco, CA.

[4] See, e.g., Zhao, Jun, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, Nigel Shadbolt. 2019. "I make up a silly name": Understanding children's perception of privacy risk online." CHI Conference on Human Factors in Computing Systems Proceedings (May):1-13. Galvan, Adriana, Todd A. Hare, Cindy E. Parra, Jackie Penn, Henning Voss, Gary Glover, B.J. Casey. 2006. "Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents" Journal of Neuroscience 26(25) (June 21): 6885-92 (teens' brain development can bias them towards risky behaviors).

[5] OFCOM. 2016. Children and Parents: Media Use and Attitudes Report. https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pd. See Zhao, Jun, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, Nigel Shadbolt. 2019. "I make up a silly name": Understanding children's perception of privacy risk online." CHI Conference on Human Factors in Computing Systems Proceedings (May):1-13 (children have "little sense of the risks posed by the accumulation of personal data over time). Galvan, Adriana, Todd A. Hare, Cindy E. Parra, Jackie Penn, Henning Voss, Gary Glover, B.J. Casey. 2006. "Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents" Journal of Neuroscience 26(25) (June 21): 6885-92.

[6] See Sampasa-Kanying, Hugues and Rosamund F. Lewis. 2015. "Frequent Use of Social Networking Sites Is Associated with Poor Psychological Functioning Among Children and Adolescents. Cyberpsychology, Behavior, And Social Networking 18, no, 7:380-5. Additional study is needed to further explore causes and correlations between technology use and well-being, depression, and suicide. Odgers, Candice L. and Michael Robb. 2020. Tweens, teens, tech, and mental health: Coming of age in an increasingly digital, uncertain, and unequal world. Common Sense Media, San Francisco, CA.

[7] Mostafavi, Beata. 2020. "Some Children at Higher Risk of Privacy Violations from Digital Apps."University of Michigan Health Lab, Sep. 8, 2020. https://labblog.uofmhealth.org/health-tech/some-children-at-higher-risk-of-privacy-violations-from-digital-apps. But see Han, Catherine, Irwin Reyes, Alvaro Feal, Joel Reardon, Primal Wijesekera, Narsio Vallina-Rodriguez, Amit Elazari, Kenneth A. Bamberger, and Serge Egelman. 2020. "The Price is (Not) Right): Comparing Privacy in Free and Paid Apps.", Proceedings on Privacy Enhancing Technologies (PoPETS) 3 (August):222-242 . https://doi.org/10.2478/popets-2020-0050.

[8] Singer, Natasha. 2019. "The Government Protects Our Food and Cars. Why Not Our Data?" New York Times, Nov. 2, 2019.

The School Zone Should Be a Privacy Zone

Privacy concerns are particularly acute in the educational space, both because of the sensitivity of the information and the context in which it is shared. Educational records often contain highly specific data, such as social security numbers, mental health assessments, and the financial status of families.[9] Indeed, both children's data and educational data are considered sensitive in their own right.[10] Further, the fiction of notice, choice, and consent that persists in the consumer context becomes pure fantasy in the educational context. Parents and students have little understanding about how technology chosen by districts and teachers may collect, process, or share information. And they rarely have a choice—actual or perceived—as to whether or not to engage with a service. Schools, meanwhile, may choose services that offer features and functionality at low prices while not considering the ramifications for students' privacy. Or they may lack the resources to fully vet programs they plan to implement for hundreds or thousands of students.[11] Schools across the country lack resources to adequately secure this sensitive information; a single breach could expose thousands of students' information.[12] And, once again, disadvantaged families are likely to suffer disproportionately as they face additional barriers to using technology.[13] This is particularly concerning given that an inaccurate educational record or algorithmic determination about ability or intelligence can have wide-ranging implications for a young person's future.[14]

The Current Crisis Exacerbates Longstanding Problems

The pandemic has pushed more people to spend more time online. Tens of millions of children in schools across the country have been forced into a virtual education experiment. The line between consumer tech and ed tech has become even blurrier, with consumer tech products designed for business use being used for preschool playgroups, often without necessary

[9] See Nowicki, Jaqueline M. 2020. "Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm." GAO-20-644. Washington, DC. Government Accountability Office.

[10] See, e.g., Ohm, Paul. 2015. "Sensitive Information," S. Cal. L. Rev. 88:1125-1196 (noting that children's information has traditionally been regarded as sensitive). Family Educational and Privacy Rights Act, 20 U.S.C. § 1232(g). Student Online Personal Information Protection Act (SOPIPA), Cal. Bus. & Prof. Code § 22584.

[11] Indeed, schools with fewer resources have sometimes been quick to view experimental technology as a cheap fix, including fully virtual charters. See Benner, Meg and Campbell, Neil. 2018. "Profit Before Kids." Center for American Progress. https://www.americanprogress.org/issues/education-k-12/reports/2018/10/10/459041/profit-before-kids/.

[12] Nowicki, Jaqueline M. 2020. "Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm." GAO-20-644. Washington, DC. Government Accountability Office.

[13] Hernandez, Martha. 2020. "Analysis: Educators Say Distance Learning Failed Most English Learners Last Spring." The 74 Million, Sep. 9, 2020. https://www.the74million.org/article/analysis-educators-say-distance-learning-failed-most-english-learners-last-spring-heres-10-ways-to-more-effectively-serve-els-as-schools-reopen-for-virtual-and-blended-learning/

[14] See Ohm, Paul. 2015. "Sensitive Information," S. Cal. L. Rev. 88:1125-1196. Families who are less familiar with technology may have children flagged by computer systems as struggling academically when the issue is truly a struggle with technology or connectivity.

protections in place. Individuals have disrupted online classes,[15] child predators have found more victims,[16] and hackers see school districts as increasingly attractive targets.[17]

The laws protecting children and students' information have not kept pace with technological changes. The Children's Online Privacy Protection Act (COPPA) was passed twenty years ago. And the Federal Education Rights and Privacy Act (FERPA) was passed in 1974, making it over forty years old.[18] These laws—FERPA especially—do not account for current technological realities, and they leave young people unprotected. In recent years, as other countries have moved to protect digital privacy for all—with special protections for minors—the U.S. response has been lackluster. States have had to take the initiative, especially in the area of student privacy, but almost one in five states has yet to put in place any modern student privacy laws addressing digital technology in schools.[19] Laws that protect young people outside of school are even more lacking, though the recent California Consumer Privacy Act, which offers special protections for children up to 16, is one counterexample.[20] State laws are an important first step, and lawmaking at the state level is generally more agile than at the national level, and can more easily keep up with shifts in technology. However, a strong federal floor would afford children equal protection and improve the regulatory climate for businesses whose products span state lines.

Congress has considered a variety of proposals—including a number of bipartisan ones—but privacy has never quite become a legislative priority. Relevant agencies have moved only haltingly on this issue. The Federal Trade Commission, which completed a rulemaking update of COPPA in 2012, has continued to enforce COPPA, including against large players (e.g., YouTube), but enforcement remains underwhelming in terms of both scope and penalties.[21] The

---

[15] Hartner, Zeke and Abigail Constantino. 2020. "Fairfax schools cancel online classes for the week for "necessary updates", WTOP News, Apr. 15, 2020. https://wtop.com/education/2020/04/fairfax-co-public-schools-cancel-online-classes-for-the-day-amid-technical-issues/.

[16] Nelson, Blake. 2020. "Online child predators more dangerous during COVID-19 crisis, N.J. officials say," NJ.com, Aug. 26, 2020. https://www.nj.com/crime/2020/08/online-child-predators-more-dangerous-during-covid-19-crisis-nj-officials-say-21-arrests-show-why.html

[17] Wisely, John. 2020, "Why hackers are targeting local school districts." Detroit Free Press, Oct. 12, 2020. https://www.freep.com/story/news/education/2020/10/12/hackers-targeting-local-school-districts-walled-lake/5965647002/. Hobbs, Tawnell D. 2020. "Hacker Releases Information on Las Vegas-Area Students After Officials Don't Pay Ransom." The Wall Street Journal, Sep. 28, 2020. https://www.wsj.com/articles/hacker-releases-information-on-las-vegas-area-students-after-officials-dont-pay-ransom-11601297930.

[18] The 1978 Protection of Pupil Rights Amendments (PPRA) was more recently updated during No Child Left Behind, but it offers only limited protections, including some opt-out rights with respect to certain marketing and surveys.

[19] Future of Privacy Forum's Student Privacy Compass. "State Student Privacy Laws." Accessed October 26, 2020. https://studentprivacycompass.org/state-laws/.

[20] California Consumer Privacy Act, Ca. Civ. Code 1798.100 et seq. (A.B. 375, 2018). Proposition 24, the California Privacy Rights Act (CPRA), which California voters backed on Nov. 3, 2020, will eventually amend and replace CCPA.

[21] Reports of privacy violations of child-directed apps are frequent. See, e.g., Lunden, Ingrid. 2020. "Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations." TechCrunch, Oct. 23, 2020. https://techcrunch.com/2020/10/23/google-removes-3-android-apps-for-children-with-20m-downloads-between-them-over-data-collection-violations. Reyes, Irwin, Primal Wijesekera, Joel Reardon, Amit Elazari. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale, Proceedings on Privacy Enhancing Technologies (PoPETS) 3 (June):63-83. https://doi.org/10.1515/popets-2018-0021.

FTC's COPPA rule review efforts, announced in 2019, have been stalled due to an unexpected flood of comments from content creators, many unhappy with or misunderstanding the FTC's YouTube case. With respect to student data specifically, the FTC held a joint workshop with the Department of Education in 2017 to address the complex question of whether and when schools can consent on behalf of parents,[22] but a promised joint report never materialized (though both have made efforts to update non-binding guidance regarding distance learning during the pandemic). The Department of Education's Privacy Technical Assistance Center (PTAC) was established in 2010 and has issued guidance on technology and privacy issues, such as on contracts between schools and ed tech providers, but it has little authority to provide necessary overhauls to FERPA or to ensure appropriate compliance from company vendors.

Putting in place strong privacy protections now will enable children and their families to safely make use of all that technology has to offer. Young people should feel free to play, learn, and grow—engaging with new, different, and even difficult ideas—without fear that their every move is being monitored or monetized. Schools should be educated and empowered to protect students' privacy and personal information. And companies should have clear rules of the road when digitally interacting with young people.

Plan of Action

Legislative Initiatives

Support Strong Baseline Privacy Legislation

Congress has shown bipartisan interest in privacy, with bills that shift privacy burdens from individuals to companies, offer protective defaults, and expand FTC authority and penalties. The White House and Federal Trade Commission should encourage Congressional efforts to pass a unified, strong and comprehensive privacy bill by identifying key components and offering public support for privacy as a priority. Any legislation should at the very least: offer effective redress; grant privacy regulators APA rulemaking, civil penalty authority, and jurisdiction over the entire online ecosystem; and provide a strong national floor for privacy standards.

Support Children's Privacy

The White House and FTC must also encourage Congress to pass strong privacy protections for youth, ideally as part of a strong comprehensive bill, or, if that is not feasible, as a standalone effort. At a minimum, protections must be extended to teenagers—ideally up to age 18—and must prohibit behavioral ad targeting to children under 13. Protections must also apply to more sites than those currently covered by COPPA; ideally sites and services likely to be accessed by

Severity of penalties has been criticized by child advocates and Commissioners themselves. See, e.g., Singer, Natasha and Kate Conger. 2019. "Google is Fined $170 Million for Violating Children's Privacy on YouTube." The New York Times, Sep. 4, 2019. https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html.

[22] Student Privacy and Ed Tech Conference, Federal Trade Commission and Department of Education, Constitution Center, Washington, DC, Dec. 1, 2017.

youth would be covered, consistent with recent UK rules.[23] And enforcement provisions must be meaningful. Models for these protections in the U.S. include the bi-partisan COPPA 2.0 and the Protecting the Information of our Vulnerable Children and Youth (PRIVCY) Act.

Buttress and Support the Federal Trade Commission

In addition to supporting expanded rulemaking authority, Congress should offer additional support to the FTC or any new regulator, including offering funding of at least $160 million for staffing commensurate with European data protection regulators.[24] At the FTC, such funding could support additional technologists and attorneys in the Bureau of Consumer Protection's Division of Privacy and Identity Protection and/or staff in a potential new technology-focused bureau.

Expand Technology Expertise at the Department of Education and in Schools

Congress should also offer additional support for expanding technological expertise at the Department of Education (ED), and funding for schools' own privacy and security initiatives. At ED, such funding could support more technologists, attorneys, and staff with a background in education in the Office of Planning, Evaluation and Policy Development, including the Student Privacy Policy Office and the Office of Educational Technology. Education agencies should be supported with additional funds to hire and train privacy and security staff and implement safeguards.

Executive Initiatives

Task Force on Students & Digital Learning

The digital transformation of students' learning requires additional consideration in order to protect their privacy. The White House should establish a task force on "Students & Digital Learning" to study technology benefits and risks, including privacy and other online harms. This should build on past stalled efforts between FTC and ED, described above, as well as Congressional efforts to modernize FERPA (including closing the directory-information loophole) and pass ed tech vendor-focused privacy legislation (such as the bipartisan Safeguarding American Families from Exposure by Keeping Information and Data Secure (SAFE KIDS) Act). The task force should include participation from the Department of Commerce, Federal Communications Commission, Bureau of Indian Education, Federal Bureau of Investigation, Department of Homeland Security, and any other needed additional experts. Some immediate goals should be to develop strong and specific privacy-protective draft legislation and updates to FERPA that apply to schools and to technology providers which collect student information.

[23] See UK's Age-Appropriate Design Code. 2020. "Services covered by the code."(This code applies to "information society services likely to be accessed by children" in the UK."). https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/.

[24] European regulators on average have 5 staffers for 1 million individuals; assuming 320 million in U.S. that is 1600 staffers and assume FTE of $100k.

The task force can also study how schools are incorporating technology and offer guidance on digital learning best practices as well as cybersecurity recommendations.[25]

Better Understand Children's Technology

Section 6(b) of the Federal Trade Commission Act empowers the FTC to conduct wide-ranging studies investigating opaque markets and industries. Previously, the FTC has used this authority to study markets including data brokers and patent assertion entities. It announced an investigation into broadband privacy in 2019. Recently, a bipartisan group of senators asked the FTC to study the children's technology market and the educational technology market.[26] Commissioners on both sides of the aisle have expressed support for 6(b) studies on the privacy and data security practices of technology companies.[27] Now, the FTC should investigate companies' data processing and practices, use and vetting of algorithms, commercial use of children's information, audience information, sources of information, consumer complaints, and advertising practices. Ed tech companies should additionally be asked about transparency with schools and parents, variations and relationships between educational and commercial products, whether and how companies obtain consent under COPPA, agreements with schools, and how parents and students can access and correct information.

Robustly Enforce A Strong COPPA Rule

Following a 6(b) study of the industry, the FTC could finish its rule review of COPPA, at least with respect to non-educational questions, which, as described above, deserve additional consideration. Future rulemaking could demonstrate the FTC's commitment to protecting children's privacy by ensuring term definitions are as strong as possible. One term of particular importance is "actual knowledge," as COPPA only applies to companies with "actual knowledge" of children on their sites (or sites "directed to" children). Actual knowledge is undefined in statute, and the rule should be explicitly interpreted in line with the standard legal dictionary definition, "[k]nowledge of such information that would lead a reasonable person to inquire further."[28] This will help prevent companies from disclaiming knowledge of children on their sites in absurd circumstances, as they do now. Rulemaking could also strengthen FTC oversight of and transparency around COPPA safe harbors.

---

[25] There has been some Congressional interest in creating school cybersecurity resources and supporting a trained cyber workforce including the bipartisan K-12 Cybersecurity Act and the Enhancing K-12 Cybersecurity Act, and a recent GAO report details security concerns at schools. Nowicki, Jaqueline M. 2020. "Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm." GAO-20-644. Washington, DC. Government Accountability Office.

[26] Markey, Edward J. and Josh Hawley, Richard Blumenthal, Bill Cassidy, Dick Durbin, and Marsha Blackburn, Senate letter to FTC, May 8, 2020. https://www.markey.senate.gov/news/press-releases/senator-markey-leads-bipartisan-call-for-the-ftc-to-launch-major-childrens-privacy-investigation. See also advocate requests, Campaign for a Commercial-Free Childhood and Center for Digital Democracy, letter to FTC, Mar. 26, 2020. https://commercialfreechildhood.org/wp-content/uploads/2020/03/6B-Letter-3.25.20.pdf. Common Sense Media, letter to FTC, Mar. 26, 2020. https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/ftc_6b_letter_1.pdf.

[27] Wilson, Christine and Rohit Chopra. 2020. Statement of Commissioner Wilson, Joined by Commissioner Chopra, Concerning Non-Reportable Hart-Scott-Rodino Act Filing 6(b) Orders, Feb. 11, 2020. https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-technology-platform-companies/statement_by_commissioners_wilson_and_chopra_re_hsr_6b_0.pd.f

[28] Garner, Bryan A. 2019. Black's Law Dictionary. St. Paul, MN: Thomson West.

Even with the current rule, the FTC should enforce all aspects of COPPA, including especially under-enforced provisions such as the requirement that companies do not collect more information than they need for a service, and that parents may consent to the collection but not sharing of a child's information.[29] The FTC should also ensure that penalties are meaningful and actually a deterrent. Fines must be large enough so that companies cannot profit from violating COPPA. Responsible individuals should be held accountable. Structural remedies must be sufficient to ensure corporate change. These are ideas that have already been raised by individual Commissioners; [30] the White House and Congress can encourage the Commission as a whole to support these efforts by providing public cover and most importantly additional resources.

Support Schools and Educators Implementing Technology

As schools and districts increasingly rely on technology for all aspects of learning and administration, the Department of Education can provide additional support to education agencies: more guidance on privacy and security best practices and legal compliance; advice for students and parents regarding rights with respect to digital records (such as access, correction and portability); privacy and cybersecurity training for education professionals; consideration of equity issues with school technology and distance learning; and additional attention to the companies and services playing an increasingly outsized role in the nation's schools.

[29] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5(a)(2) and 312.7 (2013).

[30] See Chopra, Rohit. 2019. Dissenting Statement of Commissioner Rohit Chopra, In the Matter of Google LLC and YouTube, LLC, Sep. 4, 2019. https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf. Slaughter, Rebecca Kelly. 2019. Dissenting Statement of Commissioner Rebecca Kelly Slaughter in the Matter of Google LLC and YouTube, LLC, Sep. 4, 2019.
https://www.ftc.gov/system/files/documents/public_statements/1542971/slaughter_google_youtube_statement.pdf

About the Author

Ariel Fox Johnson is senior counsel for policy and privacy at Common Sense Media. Her work focuses on enhancing family privacy rights, strengthening students' educational privacy, and promoting robust consumer protections in the online world. She frequently advises policymakers, industry, and tech experts and has helped develop student, consumer, and children's privacy laws. Ariel is a graduate of Harvard College and Law School. Prior to joining Common Sense, Ariel worked on privacy, media, intellectual property, and technology matters at corporate law firms and clerked for the Honorable Peter J. Messitte (D. Md.).

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit dayoneproject.org.