Comments from

to

United Nations
Office of the High Commissioner for Human Rights
Special Rapporteur

September 30, 2020

Call for Contributions
on Privacy and Children

Jasmine Park, Policy Fellow
Amelia Vance, Director of Youth & Education Privacy
The Future of Privacy Forum
1400 I St. NW Ste. 450
Washington, DC 20005
www.fpf.org

On behalf of the Future of Privacy Forum (FPF), we are pleased to contribute comments in response to the United Nations Office of the High Commissioner for Human Rights Special Rapporteur's call for contributions regarding the privacy rights of children. FPF is a nonprofit organization in Washington, DC, that serves as a catalyst for privacy leadership and scholarship by advancing principled data practices in support of emerging technologies.

FPF routinely provides expert testimony and comments to the US Congress,[1] federal agencies,[2] Congressionally-chartered commissions,[3] US state legislatures,[4] and legislatures around the world.[5] We also run the annual Privacy Papers for Policymakers[6] program, which brings academic expertise to members of the US Congress, leaders of executive agencies, and their staff, to better inform policy approaches to privacy and data protection. Advocates, academics, government officials, and industry representatives from around the world attend FPF programs and events, such as Student Privacy Bootcamps,[7] the Student Privacy Train-the-Trainer Program,[8] the Digital Data Flows Masterclass,[9] and the Privacy Book Club,[10] to gain the latest insight and understanding of current privacy issues. In addition, FPF was represented in the Advisory Committee of the International Data Protection and Privacy Commissioner's Conference (ICDPPC) 2019 and is active in global debates on the future of privacy and data protection frameworks. Specific to global child privacy conversations, FPF continues to participate in an informal expert working group[11] tasked with revising the Organisation for

---

[1] Amelia Vance, *FPF Testifies Before Congress on Promoting and Protecting Student Privacy*, Future of Privacy Forum (May 17, 2018), Accessed September 24, 2020, https://fpf.org/2018/05/17/studentprivacycongressionalhearing/.

[2] Federal Trade Commission, *Student Privacy and Ed Tech*, FTC, (Dec. 1, 2017).

[3] Commission on Evidence-Based Policymaking, *The Promise of Evidence-Based Policymaking: Report of the Commission on Evidence-Based Policymaking*, App. G 310, (2017).

[4] Amelia Vance, *FPF Letter to NY State Legislature*, Future of Privacy Forum, (June 17, 2019), Accessed September 24, 2020, https://fpf.org/2019/06/17/fpf-letter-to-ny-state-legislature/.

[5] Liron Tzur Neumann, *Legislating Online Conference – The Knesset, Israel Parliament*, Israel Tech Policy Institute, (Oct. 24, 2018), Accessed September 24, 2020, https://techpolicy.org.il/legislating-online-conference-the-knesset-israelparliament/.

[6] Future of Privacy Forum, *10th Annual Privacy Papers for Policymakers*, FPF, (2019), Accessed September 24, 2020, https://fpf.org/event/10thannual-privacy-papers-for-policymakers/.

[7] Tyler Park, *FPF to Co-Host Student Privacy Bootcamp with Student Data Privacy Consortium*, Future of Privacy Forum, (Jan. 3, 2019), Accessed September 24, 2020, https://fpf.org/2019/01/03/fpf-to-co-host-student-privacybootcamp-with-student-data-privacy-consortium-1-28/.

[8] Future of Privacy Forum, *Student Privacy Train-the-Trainer Program*, FPF, (2020), Accessed September 24, 2020, https://studentprivacycompass.org/tttsyllabus/.

[9] Attended by European Union Data Protection Agencies' staff and other regulators. Future of Privacy Forum, *Digital Data Flows Masterclass: Emerging Technologies*, FPF, (2019), September 24, 2020, https://fpf.org/classes/.

[10] Future of Privacy Forum, *Privacy Book Club*, FPF, (2019), Accessed September 24, 2020, https://fpf.org/privacy-book-club/.

[11] *Workshop on the protection of children in a connected world*, OECD, (October 15, 2018), Accessed September 29, 2020, https://www.oecd.org/sti/ieconomy/workshop-on-the-protection-of-children-in-a-connected-world.htm

Economic Co-operation and Development's (OECD) principles on children's privacy in the digital environment and presented on the United Nations Educational, Scientific and Cultural Organization's (UNESCO) COVID-19 Education Response Webinar.[12]

Children worldwide are engaging online to an unprecedented degree, which entails new risks and opportunities. As nations seek to develop and refine their child privacy policies, FPF provides two considerations for the Special Rapporteur's report on how privacy affects the evolving capacity of the child and the growth of autonomy, and what factors enhance or constrain this development:

- Child privacy legislation should react to actual harms, and not intuitive concerns, in order to avoid unintended consequences that may impact the rights of children to benefit from and participate in the online ecosystem (Section 1).
- Child privacy policies must consider and balance competing and evolving interests between children and other authority figures such as parents or teachers; specifically, the policies should recognize the need to foster resilience and autonomy in children by helping them develop digital skills (Section 2).

1. Child privacy legislation should react to actual harms, and not intuitive concerns, in order to avoid unintended consequences that may impact the rights of children to benefit from and participate in the online ecosystem.

Society regards childhood as a protected period in human development when children can freely explore and learn while being shielded from harm and exploitation. According to Alison Gopnik, a leader in the field of cognitive development, "childhood is an adaptation designed to let animals learn,"[13] and is integral to healthy development. Children today increasingly explore their identities and learn about the world online. In a rapidly evolving digital environment, conventional means of protecting children from harm, such as locked doors and curfews, are no longer sufficient. Therefore, our systems and policies must evolve alongside the digital transformation to extend protections for children online. One way to protect children is through legislation.

Given both the risks and opportunities of online engagement, child privacy legislation must delicately balance protecting and empowering children online. Child privacy legislation that reacts to unsubstantiated concerns rather than addressing actual harms may lead to unintended

[12] COVID-19 Education Webinar #11, *Protecting learner data, privacy and security in the global shift to online learning*, UNESCO, (May 29, 2020), Accessed September 29, 2020, https://en.unesco.org/events/protecting-learner-data-privacy-and-security-global-shift-online-learning-covid-19-education.

[13] Alison Gopnik, *How to Get Old Brains to Think Like Young Ones*, The Wall Street Journal, (July 27, 2017), Accessed March 12, 2020, https://www.wsj.com/articles/how-to-get-old-brains-to-think-like-young-ones-1499438225.

consequences. Children ought to be protected from harmful content and interactions that may hinder their healthy cognitive, social, and psychological development. However, they should also be allowed to benefit from positive content and interactions necessary for healthy development and to gradually develop resilience as they become adults. Good child privacy legislation begins with recognizing that the internet is a neutral technological tool that reflects society. Thus, policymakers must fully explore both the positive and negative aspects of this tool to develop balanced, appropriate guardrails.

Children can benefit from online engagement by accessing a wealth of news and information on topics that interest them, connecting with family and friends, and exploring and experimenting with their identities. For example, LGBTQ+ youth can connect with others in the community and be empowered by learning about relevant social, health, and political issues. Children can also find help through resources such as websites offering mental health support or allowing them to report abuse.

However, children also face serious risks online, including commercial exploitation by businesses, exposure to age-inappropriate content, threats to their physical safety by predators, loss of opportunities due to a permanent record online, and attacks on their self-esteem through cyberbullying and social media pressure. As the commodification of data increases, children are an attractive audience for businesses seeking to use their data for targeted advertisements and other marketing purposes. For example, toy manufacturers use child influencers to market their products through popular YouTube videos.[14] Worldwide, businesses spent $1.2 billion on digital advertising for children in 2019, a number expected to increase to $1.7 billion by 2021.[15]

In the physical world, parents act as gatekeepers by knowing and limiting where their children go, whom they spend time with, and what they see. However, this level of control does not always exist online. Advertisements, spam emails, mistyping URLs, or searching can expose children to pornographic content. Strangers can also contact children and sexual predators can groom them, without their parents' knowledge. Moreover, the internet can create a permanent record of children's lives, which can hinder their future academic or career opportunities. Just last year, Harvard University revoked a student's admission offer after discovering he had used racist language in tweets when he was sixteen years old.[16]

---

[14] Marijke De Veirman et al., *What Is Influencer Marketing and How Does It Target Children? A Review and Direction for Future Research*, Frontiers in Psychology, (December 3, 2019), Accessed September 24, 2020, https://www.frontiersin.org/articles/10.3389/fpsyg.2019.02685/full.

[15] PricewaterhouseCoopers, *Kids digital media report 2019*, PwC, (May 2019), 11, Accessed March 12, 2020, https://cdn2.hubspot.net/hubfs/5009836/PwC%202019/Kids%20Digital%20Media%20Report%202019%20.pdf?__hstc=135998062.d61923792d984f09a75b586a661261d6.1583863687579.1583863687579.1583863687579.1&__hssc=135998062.1.1583863687579.

[16] Scott Jaschik, *Harvard Latest Revoked Admissions Offer*, Inside Higher Ed, (June 24, 2019), Accessed March 12, 2020, https://www.insidehighered.com/admissions/article/2019/06/24/harvard-rescinds-admissions-offer-over-applicants-past-racist-writings.

Due to the human brain's negativity bias,[17] people often focus on risks more than opportunities. This disproportionate emphasis on potential harms may tempt policymakers to quickly pass strict legislation in their quest to protect children, but such legislation may ultimately compromise children's opportunities to learn, connect, and explore. We believe the US experience with student privacy legislation, particularly over the past six years, provides valuable insight for policymakers around the world seeking to develop balanced child privacy legislation.

1.1 The US Student Privacy Landscape: Unintended Consequences

Over the past decade, data protection questions have risen as US schools are increasing their reliance on online services and third-party vendors to serve students. Well over a thousand bills have been introduced in all 50 states and the US Congress since 2014, resulting in more than 130 new laws passed. Many of these laws responded to understandable fears and addressed misunderstandings of existing laws. Disputed issues included whether third-party companies could share or sell student information and both fact-based and inaccurate concerns about sharing sensitive student information such as health, discipline, or social-emotional data with state and federal governments. The laws that were reactionary and passed quickly in response to fears have often led to unintended consequences.

To provide parents with more transparency and authority over how schools collect and share their children's data, Louisiana policymakers enacted a law that required schools to obtain parental consent before sharing data outside the school. The law was vague, but had strict penalties: large fines and jail time for individuals, including for teachers who might mistakenly share protected information. Schools were afraid to share any information without parental consent. Since many parents missed or forgot the opt-in forms, schools questioned whether they could conduct routine activities without first gaining consent such as hanging student artwork in the hallway or publishing the names and photographs of students in the yearbook.[18] The most harmful implication for children was that, without parental opt-in, schools could not refer students to the state scholarship fund.[19] This particularly disadvantaged students without engaged parents or guardians. The law was amended in 2015 by allowing individual school districts to pass less stringent policies.

In New Hampshire, policymakers heard concerns about classes being recorded without teachers' permission, so they passed a law prohibiting schools from recording classroom sessions without

---

[17] Amrisha Vaish et al., *Not all emotions are created equal: The negativity bias in social-emotional development*, Psychological Bulletin (2008), 134 (3): 383–403, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3652533/.

[18] Amelia Vance and Casey Waughn, *Student Privacy's History of Unintended Consequences*, 44 Stetson U. Leg. Rev. at 536.

[19] Louisiana House Education Committee Meeting, *Testimony for Amendments to HB 718, Statement of Rep. John Schroeder*, (May 2015), Accessed September 24, 2020. http://house.louisiana.gov/H_Video/VideoArchivePlayer.aspx?v=house/2015/may/0512_15 _ED.

first gaining school board approval, a hearing, and parental consent.[20] However, the law potentially conflicted with the Individuals with Disabilities Education Act, a federal law requiring public schools to make reasonable accommodations for students with disabilities, which can entail recording classes.[21] Additionally, teacher certifications in the US frequently require prospective teachers to record themselves teaching, so the law jeopardized teachers' ability to become certified.[22] These unintended consequences prompted the legislature to amend the law the following year.[23]

Connecticut passed a law in 2016 requiring a contract between school district boards of education and all parties with whom schools shared data, to ensure that student data received contractual protections.[24] The state department of education interpreted the law broadly: even if only two students in a school district relied on a software application for their education—such as using a voice-to-text application that was not made for or marketed to schools in order to serve students with disabilities—the district would need a contractual agreement with the software vendor to comply with the law.[25] Since the Connecticut law only required districts to make these agreements but did not require vendors to adhere to the law's requirements, in particular vendors with off-the-shelf software that was intended for a general, not school audience, many districts forewent beneficial software that could have helped students. Legislators later amended the law twice to address the example above and other unintended consequences.[26]

Reacting quickly to news that a political campaign was accessing contact information from schools to text students about an election, with messages encouraging students to vote and volunteer for certain candidates before a local election in 2017, Virginia legislators passed a student privacy law the following year, requiring schools to gain consent before sharing certain basic student information, including names and email addresses.[27] Universities in the state

---

[20] H.B. 507, 2015 Sess. (N.H. 2015).

[21] Priscilla Morrill, *Law on Recording in Classroom Questioned*, Monadnock Ledger-Transcript, (Nov. 5, 2015), Accessed September 24, 2020, https://www.ledgertranscript.com/Archives/2015/11/p1Schoolsml-110315.

[22] American Association of Colleges for Teacher Education, *Privacy and Classroom Video Recordings for Teacher Preparation*, AACTE, n.d., Accessed September 24, 2020, https://secure.aacte.org/apps/rl/res_get.php?fid=2529&ref=res.

[23] H.B. 1372, 2016 Leg. Session (N.H. 2016); Amelia Vance and Casey Waughn, *Student Privacy's History of Unintended Consequences*, 44 Stetson U. Leg. Rev. at 539.

[24] Act of June 9, 2016, Pub. L. No. 16-189, Stat. 5469 (2016) (concerning student data privacy).

[25] Amelia Vance, *Speech on the Accidental Consequences of Student Privacy Laws at SXSW EDU*, (Mar. 6, 2018); Amelia Vance and Casey Waughn, *Student Privacy's History of Unintended Consequences*, 44 Stetson U. Leg. Rev. at 540.

[26] 2017 Legis. Bill Hist. CT H.B. 7207 (Conn. 2017); 2018 Legis. Bill Hist. CT H.B. 5444 (Conn. 2017).

[27] Amelia Vance and Casey Waughn, *Student Privacy's History of Unintended Consequences*, 44 Stetson U. Leg. Rev. at 543; Carmen Forman, *Progressive Political Group Obtains Cellphone Numbers from Virginia Tech*, Radford Students For Electoral Campaigns, The Roanoke Times, (Oct. 3, 2017), Accessed September 24, 2020, https://www.roanoke.com/news/politics/montgomery_county/progressive-politicalgroup-obtains-cell-phone-numbers-from-virginia-tech/article_43921646-7977-5040-b92b2db4fa1b7350.html; Paul Fletcher, *Editorial: A*

removed internal and external student directories from their websites as well as the auto-complete feature for email addresses from university emailing platforms. There was confusion about whether professors could even share student contact information so groups of students could collaborate on projects.[28] The law was later amended to correct these unintended consequences.[29]

The inefficiencies, confusion, anxiety, and actual harms students and other education stakeholders faced resulted from student privacy legislation passed hastily without adequate external input and the lack of clarity on the scope and requirements of the laws. Over the past few years, FPF has seen the growing debate around increasing child privacy protections often mirrors the past six years of debates on student privacy, without reflection on the lessons learned from privacy protections that go too far and harm children's opportunities.

1.2 Recommendations to Mitigate Unintended Consequences

Policymakers can mitigate unintended consequences by ensuring that legislative language is clear, specific, and reflects the contexts in which stakeholders will implement the laws, providing adequate training and resources, and including and proactively engaging with stakeholders from a wide array of backgrounds throughout the legislative process. Without clear and specific language, the laws can be interpreted in a variety of ways, which may result in confusion, anxiety, and unintended consequences. Terms should be carefully defined to establish a common baseline of understanding among all stakeholders and clearly convey the intent of the legislators. When language is ambiguous, policies may be enacted inconsistently, resulting in inefficiencies and potential conflicts with other laws. For instance, personally identifiable information is often defined differently depending upon the context. A child privacy law referring to personally identifiable information should clearly define the term to avoid confusion.

Without adequate training and resources, key stakeholders may not be equipped to comply with legal provisions. Policymakers should carefully assess the vastly different contexts in which the laws are expected to be implemented to ensure that the provisions are realistic and that parties are provided with the knowledge, skills, and resources needed to comply. For example, legislation requiring strict data security measures should be accompanied by funding to hire and maintain dedicated, skilled personnel.

---

sledgehammer or a scalpel?, Virginia Lawyers Weekly, (Dec. 21, 2017), Accessed September 24, 2020, https://valawyersweekly.com/welcome-ad/?retUrl=/2017/12/21/editorial-asledgehammer-or-a-scalpel/.

[28] Paul Fletcher, *Editorial: A sledgehammer or a scalpel?,* Virginia Lawyers Weekly, (Dec. 21, 2017), Accessed September 24, 2020, https://valawyersweekly.com/welcome-ad/?retUrl=/2017/12/21/editorial-asledgehammer-or-a-scalpel/; Ashlee Korlach, *Recent Virginia Law Prevents Release of Student Email Addresses, Necessitated Removal of Student Directory*, The Collegian, (Oct. 2, 2018), https://www.thecollegianur.com/article/2018/10/recent-virginia-law-prevents-release-of-student-email-addresses-necessitated-removal-of-student-directory.

[29] H.B. 2449, 2019 Leg. Sess. (Va. 2019).

Policymakers should also seek external input to account for the context in which the laws will be implemented. By including children, parents, educators, school administrators, and other community members throughout the legislative process, policymakers can anticipate the potential disparate impact of the laws on different populations, identify barriers to implementing the requirements, and gather broad support from the public. Policymakers globally can refer to the US experience regulating student privacy, where unintended consequences arose from failing to engage with diverse stakeholder groups before drafting legislation.

1.3 Global Child Privacy Policy Considerations: Potential Unintended Consequences

Below are some of the key considerations in child privacy policy discussions that should incorporate the lessons learned from the unintended consequences of student privacy laws.

A. Which Ages Should Receive Greater Privacy Protections, and Should the Parent or Child 'Own' Those Privacy Rights?

In an increasingly complex landscape of child privacy legislation globally and with the rising costs of compliance, online service providers have traditionally required age verification prior to users being able to access their services. When age verification is requested, children generally have the binary choice of either telling the truth about their age and retaining child privacy protections, but losing access to online services; or lying about their age to access to online services, but losing child privacy protections. Ideally, child privacy policies should not condition children's access to the online ecosystem on trading-off their privacy rights; instead, they should seek to protect children from actual harms while allowing them to access opportunities online. Policies should also recognize the different levels of development and readiness of children and teens, understanding that protections that are appropriate for very young children may not be for older teenagers.

In the US, the Children's Online Privacy Protection Act (COPPA), passed in 1998, requires businesses to obtain verifiable parental consent before collecting personal information from children under the age of thirteen.[30] That age was not a deeply-researched, evidence-based decision by Congress; instead, it represented a compromise. COPPA, as originally introduced, covered children under the age of sixteen, but this was opposed not only by companies, but also by civil liberties advocacy groups that argued that the parental consent requirements in COPPA could limit teen access to information that they might need, such as resources about birth control

[30] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

or getting help if their parents were abusive.[31] In other words, there was a recognition that a child's level of maturity changes, and the primary agent making decisions about privacy and access to information can and should shift in recognition of the evolving capacity of the child.

In today's discussions about child privacy happening across the world, there are many stakeholders who feel that child privacy protections should extend beyond age thirteen, and some of the proposals introduced have focused on extending those protections without acknowledging the interests of the child to be able to make their own privacy decisions as they mature.[32] However, many of the protections that have actually passed into law have thankfully recognized children's evolving capacity: for example, the California Consumer Protection Act (CCPA) requires that businesses, in addition to obtaining verifiable parental consent for children under the age of thirteen, obtain opt-in consent from teens aged thirteen to fifteen, in order to sell their information.[33] A new US federal consumer data privacy bill,[34] introduced in December 2019, would require parents to provide consent prior to any transfers of data from children under the age of sixteen and would allow parents to determine whether entities covered by the law may process their children's data, until their children turn eighteen. This provision differentiates this bill from other significant federal consumer privacy proposals, which do not contain provisions related to child privacy.[35]

As new policies and proposals emerge, it will be crucial to critically analyze and determine the most appropriate age that provides sufficient protections for children between age thirteen and adulthood. Given the progression of child development, gradually increasing rights as children age can ensure that legislation accounts for children's varying needs at different developmental stages. Teenagers, in particular, should have opportunities to exercise their agency and develop autonomy. Providing evolving rights and protections, while more challenging in practice, better accounts for children's evolving capacities and needs. Therefore, granting parents and teens joint rights gives teens more autonomy and independence and allows parents oversight and peace of mind.

Similarly, it is important to consider the confusion and difficulties that may arise when countries differ on what privacy rights children or their parents have and at what ages those rights end or

---

[31] Julie Jargon, *How 13 Became the Internet's Age of Adulthood*, The Wall Street Journal, (June 18, 2019), Accessed September 29, 2020, https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201.

[32] Preventing Real Online Threats Endangering Children Today (PROTECT) Kids Act, H.R.5573, 116th Congress (2019-2020), https://walberg.house.gov/sites/walberg.house.gov/files/PROTECTKidsAct.pdf.

[33] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.198(a) (2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[34] United States Consumer Data Privacy Act of 2019, https://aboutblaw.com/NaZ.

[35] Future of Privacy Forum, *Closer Than Apart: Comparing Senate Commerce Committee Bills*, FPF, (December 2, 2019), Accessed March 27, 2019, https://fpf.org/2019/12/02/comparing-senate-commerce-bills/.

change. Complying with different ages of consent is relatively straightforward in the physical world where activities are generally limited within national boundaries. However, given the nature of online services operating across countries, the lack of consistency around the age at which privacy rights end or change can be a significant barrier for governments, companies, parents, and children themselves. When there are discordant child privacy policies in different jurisdictions, parents and children may be unsure of which protections apply to them and at what ages. This uncertainty can lead to a belief that there are no protections, which can undermine the trust of children and parents in their legal protections, in addition to furthering the likelihood that violations of those rights will not be remedied.

There is also a burden on online service providers when there is significant variation in child privacy rights and age requirements. This variation could lead to online service providers not only having to ask for a user's birthdate, but also having to either explicitly ask their nationality or collect data on their likely location, and then confirm based on that nationality what child privacy protections–which may clash with the protections in other jurisdictions–they must adhere to in that jurisdiction prior to allowing access to their services. For example, just in the EU, the age of consent for using data on children varies, with ten countries setting the age of consent at sixteen, three countries setting the age at fifteen, six countries setting the age at fourteen, and eight countries setting the age at thirteen.[36] This burden may pose a competitive disadvantage for companies operating in states with particularly restrictive child privacy laws or result in measures depriving children and teens the benefits of using these services, as companies choose either to invest significant resources in age verification and parental consent mechanisms or abandon the market for children and age gate their services instead.

B. Should Consent-Based or Rights-Based Legislation Protect Children?

The US relies heavily on notice and consent to determine children's privacy protections, by providing parents the rights to receive notice and provide consent for their children. However, this mechanism may be inadequate, as children often lie about their age online, sometimes with their parents' assistance, to access general-audience websites and services. A survey of parents' views on their children's use of Facebook found that "Many parents know that their underage children are on Facebook in violation of the site's restrictions and that they are often complicit in helping their children join the site."[37] Without obtaining support from parents and children, the very parties the laws seek to protect may find ways to circumvent them. Relying on parental consent also poses obstacles for children whose parents or caregivers speak limited English and for unaccompanied or emancipated minors.

---

[36] Ingrida Milkaite and Eva Lievens, *Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU*, Better Internet for Kids (last updated Dec. 20, 2019), Accessed September 30, 2020, https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751.

[37] Danah Boyd et al., *Why Parents Help Their Children Lie to Facebook About Age*, First Monday, (2011), 16: 11, https://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075.

Lawmakers in the US and other countries have implemented other mechanisms beyond notice and consent. In August 2020, the UK passed the Age Appropriate Design Code, which sets fifteen standards for businesses whose products children might use, to minimize the collection of children's data and to give children and parents more agency regarding the types and amount of data collected. The code includes strong privacy settings by default; prohibits profiling, nudging, and collecting geolocation data; and requires child-friendly language in privacy notices.[38] In these ways, the code balances the burden of protecting children online by shifting some responsibilities from consumers to businesses.

The German youth protection law requires businesses to either use scheduling restrictions to ensure that content harmful to children is not available during the day, when children are typically online; to use technical methods to keep children from accessing inappropriate content, such as sending adults a PIN after age verification; or to use age labeling that youth protection software, downloaded by parents on their children's devices, can read.[39] Again, compared to the notice and consent framework, this multipronged approach means that both consumers and businesses share the burden of protecting children's privacy.

In the US, COPPA also includes child privacy protections beyond notice and consent. COPPA requires the FTC to enforce requirements "prohibit[ing] conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity and requir[ing] operators to protect the confidentiality, security, and integrity of personal information collected from children."[40] While the law includes this data minimization requirement, unfortunately it has seldom been enforced.

Under these alternative models, children's privacy protections are not conditioned on parental consent. Rather, children receive greater protections by default, thereby requiring businesses to design their services to protect children. However, this raises further questions regarding the knowledge standard. COPPA applies to businesses directed at children or with "actual knowledge" that children under thirteen use their services. Privacy stakeholders debate whether

[38] Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services: Final Version: To be Laid in Parliament*, ICO, (January 21, 2020), Accessed March 12, 2020, https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-0-0.pdf.

[39] Andreas Grünwald and Christoph Nüßing, *Youth Protection in Germany: Online Age Checks and Daytime Blackouts Ahead?*, Morrison Foerster, (May 23, 2019), Accessed March 12, 2020, https://www.mofo.com/resources/insights/190523-youth-protection-germany.html.

[40] Laura Moy, Angela Campbell, and Lindsey Barrett, *Comments of Campaign for a Commercial-Free Childhood*, (December 11, 2019), Accessed March 12, 2020, https://commercialfreechildhood.org/wp-content/uploads/2019/12/CCFC-COPPA-comments.pdf.

"actual knowledge" or "constructive knowledge" is appropriate.[41] Another approach under consideration is to assume that all users of a service are children, unless proven otherwise through the type of service, market research, or measures taken to limit children's access.[42] However, this raises questions of free speech as online service providers could feel compelled to censor content on their services that adults find "lawful and valuable"[43] to avoid potential fines or other legal consequences. Such measures would transform the online environment for all users, limiting the availability of diverse content and interactions. Chilling free speech online is also likely to disproportionately harm marginalized groups that rely heavily on information and communities available largely through online services.

Further complicating matters is that many parents oppose the government acting as the arbiter of what their children can access online. The above-mentioned study of Facebook use found that 93 percent of parents surveyed believed that they should "have the final say about whether or not [their] child should be able to use Web sites and online services."[44] Only 2 percent believed the government should have the final say. Therefore, eliminating notice and consent provisions altogether could anger constituents who may believe they no longer have individual choice. For instance, in 2011, the South Korean government passed the Youth Protection Revision Act, also known as the Shutdown Law or Cinderella Law, requiring parental consent for children under the age of sixteen to access gaming websites and prohibiting playing internet games between midnight and 6am.[45] Due to public backlash, the law was amended in 2016, allowing parents to exempt their children from the gaming curfew.[46]

Child privacy policies should reflect a workable middle ground between requiring basic privacy protections by design and default and allowing individual choice. This balance is consistent with recommendations of the National Institute of Standards and Technology (NIST) Privacy Framework, which states, "Privacy protection should allow for individual choices, as long as

---

[41] The US Federal Trade Commission (FTC) convened child privacy experts to discuss elements of the rule as part of the COPPA rulemaking process on October 7, 2019. Federal Trade Commission, *The Future of the COPPA Rule: An FTC Workshop*, https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop. During the workshop, several experts expressed different conceptions of the "actual knowledge" standard, for example, Attorney Phyllis Marcus raised the point that recent FTC decisions lead practitioners to believe that actual knowledge means "child-directed" in practice.

[42] Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services, Consultation Document*, ICO, (2019), Accessed September 24, 2020, https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf.

[43] Ashcroft v. American Civil Liberties Union, 542 U.S. 656 (2004).

[44] danah boyd et al., *Why Parents Help Their Children Lie to Facebook About Age*, First Monday, (2011), 16: 11, https://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075.

[45] Youth Protection Act, Act No. 14067, Korean Law Translation Center, (March 2, 2016), Accessed September 30, 2020, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38401&lang=ENG.

[46] Sung-mi Ahn, *S. Korea to ease online game 'shutdown law'*, The Korea Herald, (July 19, 2016), Accessed September 30, 2020, http://www.koreaherald.com/view.php?ud=20160718000987.

effective privacy risk mitigations are already engineered into products and services."[47] The path forward for child privacy legislation involves shaping guardrails that prohibit unethical practices, provide accountability, and allow parents and, when appropriate, children to determine what is permissible outside of those practices.

C. Should Child Privacy Protections be Included in Comprehensive Consumer Privacy Frameworks or are Additional Child Privacy Policies Necessary to Protect Children?

A number of countries have followed the EU's example with the General Data Protection Regulation (GDPR) in addressing child privacy protections as a part of a comprehensive consumer privacy law. Brazil's Lei Geral de Proteção de Dados (LGPD) includes a section on children's and adolescents' personal data protections. Among other provisions, LGPD requires verifiable parental consent prior to processing data of children under the age of eighteen, ensures access to services are not conditioned on providing more personal information than is necessary, and "tak[es] into account the physical-motor, perceptive, sensorial, intellectual and mental characteristics of the user" when providing notice.[48]

Thus far, the US has largely enacted standalone laws protecting child privacy, such as COPPA; and student privacy laws, including FERPA, the Protection of Pupil Rights Amendment (PPRA), and numerous state laws. However, several recent and emerging comprehensive consumer privacy laws include special protections for children. For example, CCPA also gives children special protections by requiring opt-in consent from parents for children under the age of thirteen and from teens between the ages of thirteen and fifteen. The proposed Washington Privacy Act (WPA) would also provide children with special protections as part of a comprehensive consumer privacy law, by categorizing children's data as sensitive data.

Standalone child privacy laws, much like the sector-based approach to privacy protections, are more specialized and adaptable because they address specific issues. For example, FERPA protects students' education records from disclosure without parental consent. The proposed Kids Internet Design and Safety (KIDS) Act would regulate design elements that encourage or manipulate children to spend more time on services such as YouTube and to buy certain products.[49] However, standalone laws result in a "diffuse and discordant"[50] privacy landscape in

[47] National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, NIST, (January 16, 2020), 33, Accessed March 12, 2020, https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.
[48] Law No. 13,709, of August 14, 2018 - Provides for the protection of personal data and changes Law No. 12,965, of April 23, 2014 (the "Brazilian Internet Law").
[49] Makena Kelly, *YouTube children's content faces a new threat from the KIDS Act*, The Verge, (March 5, 2020),, https://www.theverge.com/2020/3/5/21166705/youtube-kids-act-markey-blumenthal-coppa-tiktok-ryans-toy-review.
[50] Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, Columbia Law Review (2014): 583, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

which laws may conflict and leave areas unregulated. This patchwork of laws results in confusion for consumers, businesses, and governments regarding compliance and enforcement. Comprehensive privacy laws facilitate consistency in privacy protections and simplify compliance. Nonetheless, stakeholders have also criticized comprehensive laws such as California's CCPA and the GDPR for being too prescriptive and onerous.

2. Child privacy policies must consider and balance competing and evolving interests between children and other authority figures such as parents or teachers; specifically, the policies should recognize the need to foster resilience and autonomy in children by helping them develop digital skills.

The United Nations Convention on the Rights of the Child states that every child has the right to "choose their own thoughts, opinion and religion," to "share freely with others what they learn, think and feel," to "get information," and the right of privacy.[51] However, the Convention also recognizes that parents and guardians "are the main people responsible for bringing up a child," and that governments have a responsibility to help them. Many of the above-mentioned rights mention how parents and governments should help keep children from being harmed or harming others, and educate them on how to properly use those rights "in a manner consistent with the evolving capacities of the child." As discussed above, it is important to find an appropriate balance between the occasionally competing interests between the privacy rights of children and the responsibility and rights of parents or those acting in loco parentis, such as schools, to supervise their children and keep them from harm.

Children, particularly as they mature, desire and deserve the right to privacy, not only from their schools, businesses, and governments but also from their parents. Researchers have found that children vary in their conceptions of and parties from which they desire privacy based on their levels of development.[52] Young children, between the ages of 5 to 7, generally do not consider parental monitoring of their online activities as a violation of privacy.[53] However, teenagers, between the ages of twelve and seventeen, are often concerned about parental and school monitoring of their online activities.[54] Although parents and schools usually adopt these measures with the best of intentions, feeling continually watched at home and at school can impede children's healthy development of autonomy and independence. This section discusses

---

[51] *The Convention on the Rights of the Child*, UNICEF, https://www.unicef.org/child-rights-convention/convention-text; *The Convention on the Rights of the Child: The Children's Version*, UNICEF, https://www.unicef.org/child-rights-convention/convention-text-childrens-version.

[52] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, *Children's data and privacy online: Growing up in a digital age, An evidence review*, London School of Economics, (December 2018), Accessed September 29, 2020, https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.

[53] Ibid.

[54] Ibid.

these issues and offers recommendations to help children develop resilience, autonomy, and digital skills.

2.1 Parental Monitoring

To protect their children, parents are turning to monitoring programs that allow them to access their children's devices and see their files, activities, and locations—at times without their children's knowledge. There is an entire industry dedicated to gatekeeping and monitoring young people's access to the internet. Some parents install applications on their children's smartphones to track their communications, device usage, and location—trackers with similar capabilities to stalkerware.[55] Parents who adopt these technologies understandably seek to protect their children from harassment, bullying, and inappropriate content. However, this software often exposes their children's sensitive personal information to significant security vulnerabilities, and the programs operate stealthily, implying parents' lack of trust in their children.[56]

Children are keenly aware of how they are tracked online, believe that such tracking indicates fundamental issues of trust, and understand that it hinders their ability to grow freely. A student participant in one study states, "[A]ll the peers and friends I know and have talked about them being tracked for the most part think it is because their parents don't trust them. Even if a parent may not want it to come across that way, it often does."[57]

Parents should adopt such surveillance technologies only after weighing the potential risks and benefits in terms of children's privacy concerns and growth of resilience and autonomy. If parents adopt the technology, they should carefully assess whether it adequately protects their children's information from unauthorized access and includes common-sense limitations that protect children's privacy rights. Parents should also actively engage their children in the process by sharing their motivations for adopting the technology, negotiating use limitations based on their children's age and developmental stage, and being transparent about the information they access and how they will use it. In efforts to aid parents in critically assessing the potential benefits and harms of using monitoring technologies, international organizations like the UN

---

[55] Christopher Pearsons, et al., *The Predator in Your Pocket A Multidisciplinary Assessment of the Stalkerware Application Industry*, The Citizen Lab, (June 12, 2019), Accessed September 24, 2020, https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/.

[56] David Ruiz, *Parental monitoring apps: How do they differ from stalkerware?*, MalwareBytes Labs, (July 22, 2019), Accessed September 24, 2020, https://blog.malwarebytes.com/stalkerware/2019/07/parental-monitoring-apps-how-do-they-differ-from-stalkerware/.

[57] The Learning Network, *What Students Are Saying About Parental Surveillance, Living Without Wi-Fi and Vibrant Youth*, The New York Times, (March 19, 2020), Accessed September 24, 2020, https://www.nytimes.com/2020/03/19/learning/what-students-are-saying-about-parental-surveillance-living-without-wi-fi-and-vibrant-youth.html.

may find it valuable to invest in research on parental monitoring norms and the effects on child development, and provide guidance for parents.

2.2 School Monitoring

Schools have also adopted technologies such as network monitoring and surveillance cameras to prevent violence in schools and monitor students online. However, some of these practices may violate students' privacy rights and erode trust. Schools want to ensure that students have safe, productive learning environments, regardless of whether they learn in person or online. Especially in light of high-profile school shootings in the US, schools seek to prevent violence before it happens on their physical campuses.[58] Virtual learning spaces introduce new threats to students, such as cyberbullying, harassment, and exposure to age-inappropriate content online. Technology that monitors student activity online and blocks inappropriate content can help ensure that students are not endangered while on school devices or networks. Technology that monitors physical spaces, such as facial recognition tools to prevent unwanted visitors from entering campuses or video feeds that monitor student behavior, can also potentially help administrators find and address violent situations.

However, strict surveillance can erode students' trust and engender negative feelings toward themselves and their communities.[59] School surveillance measures can also complicate inequities for economically disadvantaged students, students of color,[60] and students perceived as atypical. For example, students without access to an electronic device or steady internet access could experience disproportionate surveillance simply for relying on their school-provided device or network as their only means of engaging online.[61] School surveillance also stigmatizes students exhibiting behaviors classified as threatening; one study on school violence reports that "many students who will never commit violence are labeled as potentially violent. The label itself can lead to stigmatization and, if linked with a segregated group intervention, the labeling can also significantly limit the opportunities of the identified students."[62]

---

[58] Heather L. Schwartz, Rajeev Ramchand, Dionne Barnes-Proby, Sean Grant, Brian A. Jackson, Kristin J. Leuschner, Mauri Matsuda, and Jessica Saunders, *Can Technology Make Schools Safer?*, RAND Corporation, (2016), Accessed September 29, 2020, https://www.rand.org/pubs/research_briefs/RB9922.html.

[59] Jason P. Nance, *Student Surveillance, Racial Inequalities, and Implicit Racial Bias*, 66 Emory L. J. 765 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830885.

[60] Priyam Madhukar, *The Hidden Costs of High-Tech Surveillance in Schools*, The Brennan Center for Justice, (Oct. 17, 2019), Accessed September 24, 2020, https://www.brennancenter.org/our-work/analysis-opinion/hidden-costs-high-tech-surveillance-schools.

[61] J. William Tucker and Amelia Vance, *School Surveillance: The Consequences for Equity and Privacy*, NASBE (Oct. 2016), Accessed September 24, 2020, https://eric.ed.gov/?id=ED582102.

[62] Jaana Juvonen, *School Violence: Prevalence, Fears, and Prevention*, RAND (2001), Accessed September 24, 2020, https://www.rand.org/pubs/issue_papers/IP219.html.

2.2 Recommendations on Monitoring by Parents or Educational Institutions and Providing Resources to Equip and Empower Children with Digital Literacy and Citizenship Skills

In order to balance the privacy rights and agency of children with the rights and responsibilities of parents and other adults, policymakers should engage with and bring together all the relevant stakeholders, particularly children themselves. Policymakers should recognize the evolving and, at times, conflicting rights and responsibilities of children, parents, and institutions. Parental or school monitoring of a child's device and online interactions acceptable for a six-year-old may not be for a sixteen-year-old. Policies to protect children must consider the different developmental stages and expectations of children and teens, preserving children's agency and rights.

Thoughtful child privacy legislation requires actively engaging with and soliciting input from all groups, particularly children themselves. Otherwise, the laws risk solely addressing the rights and preferences of one party at the expense of the others. For instance, unrestricted use of monitoring technologies in schools can violate students' privacy rights and impede their healthy development by signaling constant surveillance and lack of trust. Legislation that disproportionately privileges a parent's or an institution's desires over children's needs and preferences may also impede the development of autonomy. Children may resort to circumventing the laws, contributing to a further breakdown of communication and trust, to exercise their independence. Rather than limiting children's access to information and interactions online, parents and others should teach children digital literacy and citizenship skills to ensure children understand how to act responsibly and respond appropriately when they face risks online.

Rather than relying on monitoring technologies that may result in children and students feeling surveilled, parents and educators should emphasize digital literacy and citizenship skills to empower young people to make informed, responsible decisions online.

A. Digital Literacy and Citizenship Skills

Children's autonomy and independence are central to their development as fully engaged citizens. In a world increasingly mediated through online technologies and reliant on data to inform decision making, children must have the knowledge and skills to be thoughtful, active participants in online spaces. Cultivating children's digital skills not only protects their privacy but also builds a generation of global citizens who can effectively engage with and share the benefits of data and technology.

This cultivation generally occurs through educating children on digital citizenship.[63] Digital citizenship refers to an individual's ability to be active, engaged, and autonomous in determining how data and online technologies represent them. Digital citizenship depends on digital literacy, which is an individual's ability to effectively understand, interpret, and use data. Digital citizenship and literacy skills create awareness of digital rights and the role of data and technology in children's development. Among the issues that effective digital citizenship and literacy curricula cover are students' well-being, privacy, and security; identity and relationship development; responsible and respectful communication; appropriate responses to cyberbullying and hate speech; and news, media, and data reporting literacy. Digital citizenship also teaches children to understand and think critically about the information mediated through technology and their roles in that process.

Digital citizenship and literacy also relate to the growing use of data and technology for predictive analytics technologies. As these technologies require more data to improve their algorithms, surveillance of children has increased both in and out of the classroom, especially during the COVID-19 pandemic. Use of video and audio recordings during online learning and exam proctoring, attendance and location tracking, and predictive tracking and assessments all exemplify how data and technologies collect and use student data to intervene in their learning behavior and steer them toward desired institutional outcomes. However, guidance and training are lacking to help educators responsibly use this data and technologies to help their students. Without such training for students and educators, increased surveillance and algorithmic decision making may potentially harm students and drive further inequities in education.

Children should have the tools and ability to exercise their autonomy in both physical and virtual environments. By integrating digital literacy and citizenship skills into national curricula, including training and resources for children, parents, and educators, we can create a future where children benefit from digital technologies while being protected and protecting themselves from risks.

FPF recommends that the Special Rapporteur's report incorporate recommendations on developing digital literacy and citizenship skills, and encourage stakeholders to play their parts in protecting and empowering children online:

- Schools and districts can integrate digital literacy into P-12 curricula through age-appropriate, real-world, and culturally relevant materials. These programs should communicate to educators, students, and their families the benefits and risks of data use

[63] Sandra Cortesi, Alexa Hasse, Andres Lombana, Sonia Kim, and Urs Gasser, *Youth and Digital Citizenship+: Understanding Skills for a Digital World*, The Berkman Klein Center for Internet & Society at Harvard University (March 20, 2020), Accessed September 29, 2020, \https://cyber.harvard.edu/publication/2020/youth-and-digital-citizenship-plus.

and how schools and their third-party providers collect and use data. Digital citizenship and literacy curricula should also include professional development and training for teachers and staff.

- The technology industry can create age-appropriate opportunities to promote data literacy and citizenship in education products that children, educators, and parents use. They should create school-, teacher-, parent-, and child-focused information and training on the purpose of their technology and how they collect, store, and analyze data. They should also adopt ethical and equitable approaches to data use and communicate what data they use to predict which outcomes.
- Policymakers should understand and foster connections between digital literacy and citizenship and the future workforce. They should ensure that policies promote the development of children's digital skills, enabling them to participate as active and engaged citizens in a knowledge economy

3. Conclusion

As discussed above, we recommend that the Special Rapporteur's report on how privacy affects the evolving capacity of the child and the growth of autonomy, and what factors enhance or constrain this development should include a consideration of:

1. How child privacy legislation can and should react to actual harms, and not unsubstantiated fears, in order to avoid unintended consequences that may impact the rights of children to benefit from and participate in the online ecosystem (Section 1); and
2. How child privacy policies must consider and balance competing and evolving interests between children and other authority figures such as parents or teachers, and recognize the need to foster resilience and autonomy in children by helping them develop digital skills (Section 2).

In addition to these two considerations, we suggest that the report also include a discussion on the need for schools, districts, and their third-party vendors to be transparent about data and technology use, storage, analysis, and purpose with children, parents, and other relevant stakeholders. In our digitized society, the efficient flow of information is often necessary to engage in routine activities. Full participation by children and adults in the online environment requires trust; in particular, in order to fully develop their autonomy and sense of self, children must trust that they can share information about themselves—from information shared through online searches to data collected by educational applications—and have that information protected and only used with respect for the original context within which it was shared. Fostering trust is especially important for vulnerable groups, such as communities from racial, ethnic, religious, or sexual minorities, the disability community, and refugees. These groups that have experienced discriminatory application of their data in the past may be less trusting of

businesses, institutions, and governments. Privacy protections can build or preserve trust and help people be more comfortable sharing their information by mitigating risks and maintaining a balance in power between data providers and holders.

Public trust is also necessary when shaping child privacy policies. Without buy-in from key stakeholders, policies may face fierce opposition and fail to achieve policymakers' goals. A critical step in building trust when creating new child privacy protections is practicing transparency by continuously engaging with stakeholders, providing clear and accessible communications, and adopting a system for accountability.

FPF welcomes the opportunity to discuss these recommendations further and to provide additional details or action steps.