Written Testimony of Amelia Vance

Founder and President, Public Interest Privacy Center

Before the US House Subcommittee on Innovation, Data, and Commerce

““Addressing America’s Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans’ Personal Information””

Thursday, April 27, 2023

Chair Bilirakis, Ranking Member Schakowsky, and Members of the Committee:

It is an honor to testify before you on the need for better child and student privacy protections. I am the President and Founder of the Public Interest Privacy Center (PIPC) and an adjunct professor of law at William & Mary Law School. I also run the Student and Child Privacy Center, housed at AASA, The School Superintendents Association. PIPC is a pending nonprofit that equips stakeholders with the insights, training, and tools needed to cultivate effective, ethical, and equitable privacy safeguards for all children and students.

The child and student privacy legal and practical landscape is undergoing rapid, continual change. While educators and school administrators grapple with understanding and applying new technologies and data sharing practices within the classroom, new child privacy protections are being introduced in federal and state legislation on an almost-weekly basis. Since 2014, over 140 state laws have been passed that attempt to close these gaps. What has resulted is a confusing, dense, and insufficient legal landscape that leaves parents thinking that their children are protected or that there are no laws at all. And, worse, the chaos and legal gaps leave children and students vulnerable to serious harm.

In my work over the past decade, I have worked on student and child privacy with parents, local and state education agencies, researchers, privacy advocates, civil rights advocates, data use

proponents, and state and federal policymakers. These stakeholder groups can (and have) clashed regarding the appropriate balance of the use of data with sufficiently protecting privacy, but they all agree: current sectoral privacy protections are not sufficient to protect student privacy.

Today, I will share some of what I have learned in my work in this space, provide a brief overview of the current child and student privacy landscape, outline why children and students are particularly vulnerable to privacy risks, describe how current laws fall short in protecting children and students from privacy harms, and how a comprehensive consumer privacy bill could help close these gaps and create more safeguards for students and children.

Lay of the Land

Child and student privacy legal protections currently exist through a layered, often outdated, and hard to navigate patchwork of federal and state laws. The Children's Online Privacy Protection Act (COPPA) contains significant protection gaps. For example, it only applies to information *from* children under the age of 13 - a surprise to many parents who think it applies to all information about their children - and most of COPPA's protections can be, and often are, easily waived. The Family Educational Rights and Privacy Act (FERPA) provides additional privacy protections for students, but is particularly hard to understand and apply due to the additional rules that exist in statute, regulation, guidance, and other sources of law. Like COPPA, FERPA also includes significant gaps in privacy protections; while education technology is now used for attendance, personalized learning, student counseling, and other educational and administrative purposes, those companies are not directly regulated under FERPA; schools bear the burden of ensuring big tech's compliance, absent a state law. The state legal landscape is evolving at a near-impossible to follow rate, making it hard for stakeholders, including parents, schools, and companies, to understand and navigate.

Today, there is almost universal agreement among parents, educators, and policymakers at both the federal and state levels that children and students deserve better privacy protections. The next step must be to unite decision makers' understanding of what the current laws are, what gaps remain in the current legal landscape, what additional risks need to be addressed, what the possible legislative solutions are, and how to best implement those solutions without restricting children and student's access to safe online communities and opportunities.

Given this legal landscape and the vulnerabilities that remain, child and student privacy laws are long overdue for modernization and clarity, especially in light of the rapid rate of emerging technologies. However, just expanding those protections are not enough; our children deserve and need privacy protections both the day before *and* the day after they turn 18. A carefully and well-informed, comprehensive federal privacy law could help close these gaps and provide the safeguards that children and students have long-needed. However, we also know children are uniquely vulnerable to certain harms, and it is also important to create heightened protections that safeguard children from risks unique to them.

Children, Students, and Privacy Risks

Because students—especially younger children—are not fully equipped to weigh the potential benefits and risks of data collection and use, are more socially and physically vulnerable than adults, and lack experience in navigating social norms and knowing when to trust, they require special privacy protections. They also need to be protected from the more acute harms they are vulnerable to, such as opportunity loss and identity theft, that may not fully emerge until later in life.

Without proper safeguards, students' lives and futures may be irreparably altered by privacy invasions. Over the past decade, I've found that the concerns that are most often shared from parents, educators, policymakers, and students themselves can be categorized in the following ways:

Risk	Definition	How these concerns might be raised
Health & Safety	Personal or otherwise sensitive information may be revealed that could endanger students.	Is a stranger or someone dangerous able to communicate with my child or learn where my child lives?
Over-Collection & Over-Surveillance	Over-collection and monitoring of student data and online activity can have chilling effects on students.	How much information is being collected about my child?
The Permanent Record	Records of events, specifically mistakes, may be retained	Will my child's mistakes be recorded forever?

	indefinitely, potentially leading to detailed profiles that negatively impact students' future opportunities.	
Loss of Opportunity	Student data can be used to make decisions about students and, specifically, can result in denials of opportunity.	What information will be used to make determine which opportunities my child doesn't have access to?
Equity Concerns	Students have varying access to devices or internet service, has implications for safeguards in place and monitoring that occurs.	What if the information is biased? What if it is used in an inequitable way? What if my child and I can't or don't have access to the information or technology?
Age-inappropriate Content	Students may access inappropriate websites and online content.	Is my child accessing content that isn't appropriate?
Social Harm	Revelation of personal and sensitive student information can result in stigmatization and cyberbullying.	Is my child being cyberbullied or stigmatized?
Commercialization	Companies may use student data to target students with advertisements and to build student profiles.	Are companies selling my child's data or targeting advertising to them?

Whether these risks are based on student privacy being violated or just the perception that it could be, these risks are generally what underpins child and student privacy controversies and dictates the content of child and student privacy laws, regulations, and policies. The perception of unethical or irresponsible practices due to misinformation or inadequate communication can result in a loss of trust, particularly in the student privacy context.

When we don't properly safeguard against these risks, it can result in disastrous outcomes for students that can last long after they graduate. For example, recent data breaches in

Minneapolis and Los Angeles school districts revealed sensitive information of both current and former students, including student disciplinary and health records. While increasing data security is one method of protecting against data breaches, minimizing the data that is collected in the first place and creating processes for deleting data when no longer needed can lessen the impact of these types of breaches.

The vast amount of data collected about children also poses a unique risk to children, potentially impacting their mental health, physical safety, and future opportunities. Especially in school, many children are unaware what is monitored and who may have access to their information. For example, a national survey indicated that school monitoring negatively impacts student mental health because students are concerned about expressing their opinions or seeking out resources out of fear that their searches, identities, and opinions may be revealed to others without their consent. Students' sensitive information could be better protected by limiting this type of data from being collected, restricting who has access to the data, and providing students and parents with transparent policies.

Often, current child privacy law permits almost all protections of childrens' data to be waived by consent. This is a problem because companies face few restrictions on using data after receiving parental consent. For example, parents may rush through or not read a privacy notice and consent to their child's data being collected without understanding the potential consequences. Consent is not a panacea for adequate privacy protections: consent mechanisms alone may be insufficient if students and parents do not fully comprehend what they are consenting to due to the form in which the information is conveyed, or if students' opportunities to engage in learning or activities is conditioned on use of certain tools. Many educational activities take place without consent, and, in the educational context, obtaining meaningful consent might not be feasible. Therefore, it is vital for law to include underlying privacy protections that cannot be overridden by consent or that require a higher standard of consent where the risks are clear and consent is better informed, in order to protect the privacy and retain the trust and goodwill of students, parents, and educators.

These harms are certainly concerning for any parent and may spark a knee-jerk reaction that entails keeping their kids offline all together. However, in this day and age, robust technology use is not only a reality, but also a necessity in order to prepare young adults to navigate a digital world. Let's not forget that there are also many benefits that technology has provided for children. Unable to connect with their friends and communities in-person during the pandemic,

young people relied on social media and other online tools to play, build community, explore their identities, and participate in civic and political forums. Many educational technology (EdTech) tools play a valuable and innovative role in a child's learning, digital citizenship prepares them for the adult world, and safe online interactions with their peers can create a vital sense of community. Online spaces can also be integral to fostering creative expression and providing resources related to health and well-being.

Allowing opportunities for youth online while mitigating risks is no small endeavor; it is entwined with children's well-being today and their opportunities tomorrow. In the same way we teach our children to look both ways before crossing the street, we must equip kids to make good privacy decisions for themselves. The most basic way technology changes society is through the choices that we make- the choices that *our children* make - about which technologies we adopt and reject, and how to wisely use the ones that are selected.

The current legal landscape, consisting of both federal and state level laws, does not adequately address these risks. While providing some privacy protections, significant gaps still remain.

Legal Landscape

Federal Laws

The Family Educational Right and Privacy Act of 1974 (FERPA) provides students with access to and transparency regarding their education records, and limits disclosure of education records by educational institutions to certain, limited circumstances listed in the statute. However, FERPA has a critical gap in privacy protections. FERPA applies only to schools, and therefore its restrictions and requirements only apply directly to schools, and not to private sector organizations, including EdTech companies. However, EdTech companies can be indirectly regulated under FERPA. EdTech companies are generally only regulated by FERPA so far as the contract between the school and EdTech company includes FERPA protections - something that is often a difficult burden for small schools to negotiate into contracts on their own.

In addition to FERPA, children's data is protected via the Children's Online Privacy Protection Act (COPPA), which restricts "online operators" from collecting data from children under the age of 13 without obtaining verifiable parental consent. COPPA generally only applies to online operators who target their services to children or who have actual knowledge they are collecting

information from children. As you can imagine, this actual knowledge standard creates a confusion about whether or not data collection on many sites is actually covered. COPPA also does not provide any substantive rights to children or their parents regarding the data collected.

COPPA's only protection is to apply restrictions to data collection (by requiring consent) but once the data is collected, the company has no restrictions under COPPA to how it must use, process, or share, or refrain from using, processing, or sharing the data, and it does not afford any rights in the data.

There is also massive confusion around and problematic gaps in FERPA and COPPA's protections depending on where and for what reason an app is being used by a child: if an educational app is being used in the classroom or at the direction of a teacher for homework, the data being collected is generally protected under FERPA. However, the moment that that child starts playing with that educational app for fun or at their parents' behest, FERPA ceases to apply. At that point, it would be great if COPPA covered that gap; however, since COPPA allows parents to waive many of its protections via parental consent, parents may not realize that their child is now unprotected under both FERPA and COPPA.

Misunderstandings about the intersection of FERPA and COPPA also creates problems. For example, some EdTech companies have begun to shift their COPPA responsibilities for obtaining verifiable parental consent to schools, even though companies, not education institutions, are subject to and responsible for complying with the law. Lack of clarity on the intersection between the two laws has resulted in confusion, diffusion of responsibility, and evasion.

State student privacy laws and child privacy

Since 2013, policymakers have introduced nearly one-thousand student privacy bills in all 50 states, and 41 states and Washington, DC, have enacted more than 130 laws, whose scope and effectiveness vary by state. Unfortunately, state-level student data privacy laws have been fragmented and variable, creating robust student data privacy protections in some states and insufficient protections. We've seen well-intentioned laws that have critical loopholes, and others that go too far and have overly-restrictive unintended consequences, which negatively impact student success and well-being.

For example, Louisiana passed a law that required parents to return a consent form to share any student data. Children of parents who forgot to return the form or chose not to, were

excluded from consideration from the state scholarship fund. New Hampshire similarly passed a law with good intentions but negative unintended consequences when it banned the recording of classroom lessons. Classroom recordings are sometimes necessary for students with learning disabilities so they have the resources necessary to keep up with their peers. In an attempt to protect students, New Hampshire inadvertently took this resource away from the students who need it most.

As I noted in my Seton Hall Legislative Journal article, "Student Privacy's History of Unintended Consequences," many state level laws "were passed hastily in response to public fears or specific incidents, with little stakeholder input. Others neglected to clearly define the scope and requirements of the laws, resulting in confusion and anxiety." These state experiences with passing, implementing, and fixing student privacy laws may be valuable in informing the process of improving consumer privacy protections.

State consumer privacy laws and child privacy

Utah's law includes children's privacy within its definition of "sensitive personal information," and states that controllers (covered businesses) may not "process sensitive personal data without "processing the data in accordance with" COPPA. If you are a covered business under Utah who collects information from children, but are not an online operator (or, if you have a website but don't collect data through your website), this is puzzling, because you are not required to process data "in accordance with" COPPA or to obtain parental consent since you are not an online operator. Similarly, Virginia's law also includes data collected from individuals under 13 in its definition of sensitive data, and requires businesses to not process "sensitive data concerning a known child, without processing such data in accordance with" COPPA. Like Utah, this is a bit confusing, because not all businesses that are covered under the VCDPA that collect/process child data are required to comply with COPPA. Accordingly, for businesses that are not online operators within COPPA's purview, collecting data "in accordance with" COPPA would likely look like normal data collection with no heightened protection, which undermines the purpose of these laws.

As mentioned above, these provisions are not always effective, and can be confusing, since COPPA only applies to online operators and the state consumer privacy laws apply to all businesses, regardless of how they collect information. Virginia and Utah's laws (and they are not alone) demonstrate both a misconception, and a gap when examining how state consumer privacy laws protect (or do not protect) children. The requirements in these laws seemingly try to

create a heightened collection standard when it comes to child data, similar to the heightened standard (often opt-in, rather than opt-out consent) required to collect health data, biometric data, and other similarly sensitive data, but by tying this collection standard to COPPA, which only applies in the limited context of online data collection, it does not afford the robust protection it may appear to at first brush. Legislators need to remember that not all businesses are required to comply with COPPA, so the requirements to collect data in accordance with COPPA can be confusing or ineffective.

Finally, the safe harbor offered under some state laws (such as Virginia's) which deem businesses who "comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.)" to be in compliance with "any obligation to obtain parental consent" under the law may be more workable to blend COPPA and existing state law together in a way that understands what protections COPPA is already affording and where it does not afford protections.

Some of FERPA and COPPA's gaps are also filled by state consumer privacy laws that are being introduced and passed throughout the country and affording consumers in states who have passed such laws baseline privacy rights. Beyond simply being notice and consent regimes, which is largely what COPPA is and which often does not facilitate meaningful privacy protections, these state laws go a step beyond and provide more substantive, baseline rights to individuals.

The baseline rights appearing in state consumer privacy laws generally include the right to access information, the right to know what information is being collected, the right to delete information under certain circumstances, the right to opt-out of certain uses of information (such as using information for cross-context behavioral advertising or targeted advertising), and certain rights regarding sensitive personal information (such as the requirement for the business to obtain opt-in consent prior to collection or consent for certain uses of sensitive personal information). When these laws include new child privacy protections, they generally do so by placing COPPA-like restrictions on information collection from individuals under the age of 13, by providing safe harbors for companies that collect information "consistent with COPPA's requirements," or by including information of or related to individuals under the age of 13 in the definition of sensitive personal information.

Since these laws are based on a common misconception of COPPA's breadth, they do not adequately fill the gaps that exist under current law. However, because these laws apply to all

individuals and do not set a floor for the age at which a consumer gains rights under the statutes (i.e., only afford individuals over 18 rights under the statute), these laws provide some additional protection to children via the substantive rights they afford to all consumers. Other than requiring notice of the company's privacy practices, and the right to review information collected (and in some instances, prevent further use), COPPA does not afford children (or parents on behalf of their children) significant rights in their data post-collection.

Another way that state consumer privacy laws tend to contemplate children is by including information of or related to individuals under the age of 13 in the definition of sensitive personal information. This means that the additional protections afforded to sensitive personal information under the law, which most often include opt-in rather than opt-out consent to collect and to use data for certain purposes, applies to children's data. In some ways, this is more protective than COPPA since COPPA only applies to information collection, and does not afford meaningful substantive rights or meaningfully restrict use or collection after consent to collection.

Some state consumer privacy laws say that if you are compliant with COPPA's verifiable parental consent (VPC) requirements then you also meet the requirements of the state law. However, the application of VPC can also be problematic. Obtaining VPC often involves using age verification methods, which can be easily circumvented by children. When applied, VPC may also lead to "age gating" the Internet and attempting to block certain content from children (which again, can be easily circumvented) instead of simply making the content more appropriate for audiences that may include children or younger individuals.

Instead of relying on restrictive systems that require opt-ins and parental consent, some states are moving toward a system where privacy protections are designed into the sites they expect children to visit.

Moving Away from Notice and Consent to Underlying Protections: The Age Appropriate Design Code

In one of the first meetings of the OECD's expert working group to revise their recommendation on protecting children online, Baroness Beeban Kidron presented about the Age Appropriate Design Code (AADC) and put forth the question (paraphrased here) "What if kids didn't have to lie on the internet to be protected but also get access to services?" The AADC is designed to enable children to do just that. It is built upon implementing additional safeguards that allow children to use the internet in an age- and developmentally-appropriate way.

When introduced in 2020, the United Kingdom adopted the AADC, a detailed set of fifteen non prescriptive standards "seek[ing] to protect children **within** the digital world, not protect them from it." The code establishes the following fifteen standards as a framing through which companies implement age appropriate design into their online services: best interests of the child; data protection impact assessments; age appropriate application; transparency; detrimental use of data; policies and community standards; default settings; data minimisation; data sharing; geolocation; parental controls; profiling; nudge techniques; connected toys and devices; online tools.

The EU's General Data Protection Regulation (GDPR) served as a foundation upon which the AADC is built. As explained in the Information Commissioner's foreword to the final Code, "The code is not a new law but it sets standards and explains how the [GDPR] applies in the context of children using digital services." This is a crucial point: the AADC's enhanced protections for children are based upon the foundation of privacy protections for everyone. These enhanced protections for children elevated the baseline protections to be more effective at protecting children because they accounted for children's unique vulnerabilities and need for additional protections. The US also needs a comprehensive privacy law upon which to build out additional protections for children.

The AADC includes various privacy safeguards by design and default to make the internet a safer place for children. For example, it protects the privacy of children's location data by requiring geolocation data collection be turned off by default in most circumstances and that geolocation be turned back off after a child has turned it on. It emphasizes just-in-time notifications to ensure that children are aware of what is happening while they are using the internet. It also prohibits the use of dark patterns to the detriment of children; limits profiling a child by default; requires businesses to think carefully and document decision-making about the privacy impacts of their services that are likely to be accessed by children; and calls for privacy policies to be available in terms that children can understand. Many of these child privacy protections should be represented in US privacy law, and not just to protect children.

Child Privacy-Specific State Laws

As with student privacy, policymakers have also attempted to close sectoral privacy law gaps by introducing additional state-level child privacy laws.

The U.S. Version of the Age-Appropriate Design Code

Following California's groundbreaking consumer privacy laws, California decided to innovate on child privacy too. Building off of the UK's AADC, the California Age-Appropriate Design Code Act (ADCA) mandates that businesses, as defined under the California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), implement increased privacy protections by design for online services likely to be accessed by children. These laws are based on the acknowledgement that online engagement is a reality and baseline protections must be in place. UNICEF's "Growing up in a Connected World" report demonstrates this reality. They report that across the world, one in every 3 people online are kids and teens.

The ADCA requires covered businesses to either "estimate the age of child users with a reasonable level of certainty appropriate to the risks" or to "apply the privacy and data protections afforded to children to all consumers." This requirement alone has the potential to transform how everyone, including adults, experiences the internet. As was seen with the CCPA/CPRA, because of California's size and market power and because of the breadth of the law, even with its threshold requirements, this law could change online practices for companies throughout the US because of California's market power and size. The law may also raise the baseline standard for everyone who uses the internet or online resources because if businesses can't find a way to accurately identify children, the ADCA will effectively require them to treat everyone accessing their websites as a child, which resets the baseline and could result in content restrictions, limitations on personalization, and limited functionality for all website users, when these restrictions may only be appropriate for certain content that is unsafe for children.

However, some states are choosing a more restrictive approach, passing laws that place significant restrictions on certain websites and mobile apps, such as social media platforms, related to child users of these platforms, following the example of other countries like China and South Korea. For example, Utah's law applies to minors under the age of 18, and limits how and when children can use social media by setting a curfew that prohibits evening or early morning access, and requires parental consent for use, gives parents broad rights regarding access to accounts, and places use restrictions on social media companies related to children including prohibiting social media companies to display ads to children, target or suggest groups, products, posts, or services to children, and prohibiting the use of addictive design with child users.

While this law was passed with good intentions, blocking the internet from children instead of teaching them how to safely use the internet, or making the internet safer, would have more

beneficial impacts, particularly since children historically figure out ways to bypass or circumvent age gates and access the content without consent (and in this case, past curfew). The law also treats all individuals under the age of 18 the same way, which overlooks that content that is safe and potentially beneficial for a 16 to 18-year-old is different from the content that is safe and beneficial for a four year old.

South Korea's law may actually be a case study in the problems with this approach. When South Korea passed the "Shutdown law" that banned children under the age of 16 from playing computer games between midnight and 6am, their government was, similarly to current U.S. concerns had some similar concerns to what we are hearing in the US now: worries about "internet addiction" that so bad, in some cases, that it led to people neglecting themselves or their children to "the point of death." The paternalistic law did not allow parents the flexibility to choose to allow their child to play. However, South Korea repealed the law in 2021, choosing a more balanced approach that allows parents and guardians to "arrange approved play times" instead. South Korean Deputy Prime Minister and Education Minister said that, "In the changing media environment, the ability of children to decide for themselves and protect themselves has become important more than anything," and the government would, instead, "work with related ministries to systematically support media and game-use education at schools, homes, and in society so that young people can develop these abilities, and continue to make efforts to create a sound gaming environment and various leisure activities for children."

Other bills have proposed overly restrictive requirements that fail to consider the potential impact on schools and children. For example, some proposed solutions inadvertently undermine the goals of a bill by including censorship mechanisms restricting access to certain content. These may discourage minors from seeking help and finding helpful resources that include personal stories from peers. Overly restrictive proposals may also undermine the abilities of schools to provide education using technology.

When it comes to safeguarding our children online, we commonly use two approaches. The first, encouraging our kids to wear their virtual seatbelts and take steps to stay safe while online. The second approach is to avoid the internet entirely or limit access only to occasions where there is parental supervision. Unfortunately, both approaches have significant drawbacks. They involve numerous gaps, can be easy for kids to get around, inappropriately place the onus on parents to adequately vet a technology's privacy practices, or rely on a large amount of additional data collection about families. These approaches also fail to adequately deal with

additional risks, such as commercial exploitation of their data and excessive government surveillance.

A Comprehensive Law

Comprehensive consumer privacy laws provide necessary baseline privacy protections for all consumers, including children. By providing blanket rights for all consumers, we help close many of the privacy gaps in child and student privacy laws and make technology use much safer and beneficial for children. In the same way, the UK's AADC would not be effective if it were not based on the EU's general consumer protection code, the General Data Protection Regulation (GDPR).

While providing baseline privacy rights for all consumers, a general consumer privacy law does not completely close the gaps in child and student privacy laws. Since it does not fully address the specific child privacy risks that we have laid out and for that reason, additional privacy protections for children are necessary.

Businesses must also be transparent about what data they collect, how they use it, and how individuals can exercise their afforded rights.Transparency is a fundamental principle in many privacy laws, particularly because a lot of privacy laws are premised on the concepts of notice and consent. Transparency makes consumer consent more meaningful because consumers have clear notice. However, transparency may not be enough to ensure children are protected online.

The current model for providing transparency - namely, providing a privacy notice - requires individuals, including children, to be willing and able to engage with the organization's privacy information (source: Data protection impact assessments). In reality, children (and even some adults) will not read an entire privacy notice regardless of whether it is transparent and written in an understandable way. To ensure children are protected even if they do not engage with transparent privacy policies online, additional safeguards are needed. These additional safeguards may include measures such as meaningful use restrictions and limitations specifically targeted to alleviate specific harms to children, as discussed above, or additional processing restrictions including mandatory DPIAs before processing any child information.

Certain information processing activities pose different risks and harms to children than to adults, and it is important to recognize and account for additional potential impacts on children. Conducting Data Protection Impact Assessments (DPIAs) and Algorithm Impact Assessments

(AIAs) can help identify and assess a variety of risks, including risks that are unique to children. The UK Information Commissioner's Office (ICO's) DPIA framework set forth in the AADC lends a helpful framework, identifying several child-focused risks and potential impacts, specifically saying to consider "whether the processing could cause, permit, or contribute to the risk of: physical harm; online grooming or other sexual exploitation; social anxiety, self-esteem issues, bullying or peer pressure; access to harmful or inappropriate content; misformation or undue restriction on information; encouraging excessive risk-taking or unhealthy behaviour [sic]; undermining parental authority or responsibility; loss of autonomy or rights (including control over data); compulsive use or attention deficit disorders; excessive screen time; interrupted or inadequate sleep patterns; economic exploitation or unfair commercial pressure; or any other significant economic, social or developmental disadvantage." Due to the additional vulnerabilities of childrens, it is crucial that considering the likelihood and severity of potential risks and harms of processing on children at all ages and development stages is built into the evaluation process of online technologies in addition to the considerations for all consumers in a comprehensive law.

Once potential risks and harms to children have been identified through DPIAs and AIAs, those risks and harms can then be addressed with appropriate mitigation measures to better protect children. Additional security requirements, including mandated training and appointment of privacy and security officers, can be implemented to protect the rights of children. Data minimization requirements and additional protections for sensitive data, such as requiring affirmative express consent before transferring sensitive data about and from children, are especially critical to protect children from the potential negative impacts of collecting large amounts of sensitive data about and from children.

A comprehensive consumer privacy law should prohibit businesses from using manipulative design choices (dark patterns) to obscure or impair people's ability to exercise their rights. Dark patterns (referred to as "nudge techniques" in the AADC) can cause individuals, including children, to reveal more information than they would have if a website or platform did not push them to share additional information.

Children face additional unique risks from dark patterns when compared to adults. For example, dark patterns encouraging children to overshare personal information online may result in cyberbullying and dark patterns encouraging continued use of social media may result in amplified mental harms due to the tendency of children to be more susceptible to comparing

themselves to others or viewing themselves under a microscope. Additionally, nudge techniques that encourage children to provide unnecessary personal data or to turn off privacy protective controls so that organizations can collect additional data from them goes against data minimization principles and can create a larger dossier of information related to children that can follow them for the rest of their lives.

However, manipulative design techniques can also benefit kids by gently encouraging them to stay engaged with healthy, productive, and learning-based content. For example, dark patterns or nudge techniques used in certain contexts may encourage children to share information that supports their health and wellbeing with appropriate parties to act on that information. Another potentially beneficial nudge specifically applicable to children may be techniques that encourage children to pause their activity online and step away from technology without losing progress to promote taking breaks in periods of uninterrupted screen time. In certain contexts, manipulative design techniques can be utilized in positive ways to promote childrens' wellbeing, encourage healthy habits, and encourage kid's engagement in productive activities. Because manipulative design techniques may benefit children when used appropriately, a comprehensive privacy bill should not ban them entirely. Rather, businesses should be restricted from using these techniques to keep individuals from exercising their rights, such as opting out of data collection.

A comprehensive and carefully crafted consumer data protection law can also add protections against entities and data practices less often considered to be harmful by regulating non-profits. Including non-profit organizations is useful for filling the gaps left by many existing sectoral privacy laws that do not apply to non-profit organizations.

A comprehensive consumer privacy law can also better protect data used for research. For background, many types of research—including education research—are controlled by Institutional Review Boards, which ensure that research is ethical and data is protected. However, Institutional Review Boards are rarely equipped to evaluate privacy and security risks. Ideally, a comprehensive consumer privacy law could help remedy this gap by requiring additional privacy and security specific guidelines for research, with special attention to projects that are exempt from the review process.

In addition to raising privacy protections for all consumers, a comprehensive consumer privacy bill can carve out additional protections for children that fill the gaps in existing legislation. The law would ideally apply these additional protections when the covered entity knows the

individual is under 17, without carving out different knowledge standards for some social media companies and large data holders.

Prohibiting targeted advertising to minors is a useful protection that can be provided by a comprehensive privacy bill. California's law provides this protection by allowing all consumers regardless of their age to limit the use of the "sale" and "sharing" of their data (with the "sale" and "sharing" of data generally understood to encompass the practice of targeted advertising). Specifically, California graduates the protections in this space by requiring opt-in consent from parents of children younger than 13 and directly from individuals age 13-16 in order to "sell" or "share" their personal information, and by allowing individuals over age 16 to opt-out of this practice.

Companies using targeted advertising exploit children's data to manipulate their decision-making to buying products or services, a particularly dangerous practice due to the increased vulnerability of children. This prohibition also fills gaps left by COPPA, where targeted ads are not prohibited as long as the provider has parental consent to collect and process a child's data. Additionally, the prohibition on transferring minor's data to third parties absent affirmative consent gives minors and parents control over how their data is used and limits the ability to use data for secondary purposes beyond what the data was originally collected for.

Among the provisions that require additional protections for minors, requiring large data holders to conduct yearly algorithm impact assessments that must describe, among other things, how the entity will mitigate harms specific to minors could be extremely beneficial. Requiring yearly algorithmic impact assessments to assess and mitigate potential harms to minors is a powerful tool to ensure that large data holders will think about the needs and specific vulnerabilities of children in designing and continuing to provide access to their services in safer ways for children. Entities must acknowledge the unique potential risks of algorithms to minors and plan accordingly to mitigate those harms.

Additionally, a comprehensive consumer privacy bill can create additional resources at the FTC dedicated to children and minor's privacy, including requiring the FTC to promulgate new COPPA rules and funding a new Youth Privacy and Marketing Division. The FTC has limited resources to dedicate to protecting children because they are responsible for over 70 different laws. Adding a new division dedicated to children is useful to ensure compliance with ADPPA and its minor specific provisions.

Finally, rights provided to individuals are only meaningful if they can be enforced. A comprehensive consumer privacy law can fulfill this requirement by including a private right of action for individuals to enforce their rights. A private right of action provides specific benefits to children by filling gaps in existing legislation. Parents and children cannot sue businesses that violate COPPA and must rely on the FTC and state attorney generals to enforce their rights. A comprehensive consumer privacy bill that includes a private right of action gives parents, children, and all consumers more control over their data by allowing them to enforce their rights against businesses that fail to protect them.

Including Special Protections in a Comprehensive Consumer Privacy Law for Education

While it's the best next step in protecting children and students, it's important to note that a comprehensive consumer privacy bill on its own doesn't provide all the protections we'd like to see for children and students. Consumer privacy might not clearly address the relationship between schools and companies.

In the education context, consent is often not useful. Much student data collection, use, and sharing is involuntary: children are required to attend school, where they participate in activities that generate new data about them, such as completing online homework assignments.Under FERPA, schools are permitted to consent on behalf of parents–assuming specific privacy safeguards are in place–to enable nearly every aspect of tech-supported education, from keeping attendance records to grading exams. If this changed, any student whose parents have objected would likely be unable to use EdTech. Teachers may have to choose between creating and implementing multiple lesson plans for the same classroom or not using EdTech at all. This change would leave teachers not only ill-equipped to teach in a modern environment, but also coping with post-pandemic challenges like learning loss with resources of the 1980's. It is important to protect the ability of schools to use technology as core curriculum–the digital equivalent of a textbook–without permitting opt-outs. However, in order to ensure that companies are adequately protecting privacy, additional safeguards tailored to the education context are necessary. Even where consent may be appropriate, students and parents are often not in the best position to assess the benefits and risks of data collection and use; the burden of vetting the technology used by their child's school should not be placed on them.

One way to fix this is to include a federal version of the prominent state student privacy law regulating vendors, SOPIPA, in a comprehensive consumer privacy law. For example, a draft bill introduced by Representatives Polis and Messer in 2015 included the necessary nuance to deal

with privacy in the education context, and was endorsed by most major education groups and the National PTA.

Conclusion

Children and students face many specific and acute privacy risks in this digital age. Despite policymakers' best attempts, we currently have a patchwork system of laws and protections that do not sufficiently protect children and students. Significant gaps remain in the federal laws and state laws are not successfully closing those gaps. A broader, general consumer-based approach, coupled with additional child-specific provisions, could be an effective best next step forward and a way to ensure that all children and students benefit from the opportunities provided by emerging technologies in a safer, more privacy-protective way.