Protecting Kids Online: Challenges and Opportunities in a Digital World

March 29, 2022

California State Assembly

Privacy and Consumer Protection Committee
Arts, Entertainment, Sports, Tourism, and Internet Media Committee

Amelia Vance
Founder and President
Public Interest Privacy Consulting
avance@pipc.tech

Good afternoon Chair Gabriel, Chair Boerner Horvath, Vice-Chair Kiley, Vice-Chair Valladares, and members of the Privacy and Consumer Protection Committee and the Arts, Entertainment, Sports, Tourism, and Internet Media Committee. Thank you for inviting me to testify today.

My name is Amelia Vance, and I am the Founder and President of Public Interest Privacy Consulting, an Adjunct Professor of Law at Penn State and William & Mary Law School, and co-chair of the Federal Education Privacy Coalition. I am an expert on child and student privacy law and policy, supporting county offices of education, government agencies, policymakers, non-profits, and companies on legal protections and actionable best practices to ensure the responsible use of child and student data. I also currently serve on the Organisation for Economic Co-operation and Development expert group drafting guidance for the new Recommendation on Children in the Digital Environment.

The focus of my testimony is the privacy risks that need to be addressed when designing new child privacy laws; the importance of embedding privacy in K-12 education; how privacy is an essential component of children's wellbeing; and how policymakers can

create evidence-based laws that strike the right balance between privacy protections and the opportunities that technology can support.

How can we define privacy? Privacy is recognized as a fundamental right in our Constitution and in many of California's laws. We know that privacy can include a person's control about how their personal information is shared. Privacy is subjective: what feels invasive or unnerving to one person may be innovative or desirable to another. Privacy is contextual: the information we share varies depending on if we are sharing with our partners, our children, our colleagues, or our doctors. When we share information, we expect that the context in which we share that information will be respected; for instance, that your medical conditions will not be posted to your doctor's social media account.

More and more frequently, the word "privacy" is used as a proxy for fairness. We often do not get a real choice about how information is used by governments, schools, and companies. The more information that one person or organization has about another, the more that party may influence or exert power over the other. Privacy protections give us rights that can empower and work to correct those power imbalances.

Privacy harms can be much more potent for children. As I've talked to thousands of stakeholders, I have found that concerns about child privacy can be boiled down to these risks:

Risk	**Questions parents might ask about this risk**
Safety	Is a stranger or someone dangerous able to communicate with my child or learn where my child lives?
Over-Collection & Over-Surveillance	How much information is being collected about my child, and is it necessary to collect it?
The Permanent Record	Will my child's data be deleted after a reasonable amount of time, or will their mistakes be recorded forever?
Loss of Opportunity	Will this information be used to deny opportunities to my child?
Equity Concerns	How can I prevent harms to my child from biased information or inequitable algorithms? What if we do not have access to technology or services which are expected or required?

Age-inappropriate Content	Is my child accessing inappropriate content??
Social Harm	Is my child being cyberbullied or stigmatized?
Commercialization	Are companies selling my child's data or targeting them with advertising?

These risks can be further exacerbated if we only think about a "stereotypical student" when creating programs or policies.

For example, we must consider:

- Children with disabilities;
- Children who are LGBTQIA and have a family who would harm or kick them out if they knew;
- Children facing abuse at home;
- Children with a parent who died from COVID;
- Children whose parents are working three jobs;
- Children who are undocumented, or whose families are undocumented;
- Children experiencing homelessness;
- Children who may need to share their devices with family members; and
- Children who may not have access to the internet or may have metered or slow internet.

These children must be part of our policymaking. We cannot assume that parents[1] universally have time to research privacy-protective apps, or that families will trust the government to make privacy decisions on their behalf.

Policymakers all over the world are wrestling with how we can equip today's children to access technology's benefits and minimize risks. There are many benefits: due to the pandemic, almost all students accessed their education virtually. Unable to connect with their friends and communities in person, young people relied on social media and other online tools to play, build community, explore their identities, and participate in civic and political forums. 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.

[1] The term "parents" should be read to be inclusive of parents, guardians, and other caregivers.

Digital literacy cannot be an afterthought or just one week of curriculum in a school year. 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 will change society is through the choices people make- the choices that *our children* make - about which technologies we adopt and reject, and how to wisely use the ones that are selected. Schools should provide students with tools for having thoughtful conversations and making thoughtful decisions about privacy, both online and offline, with their parents, teachers, and peers.

For example, the MIT Media Lab created a middle-school curriculum on AI, ethics and privacy.[2] It focuses on relatable examples - such as a module on redesigning YouTube, where students identify the various stakeholders that YouTube impacts and highlights where those stakeholders' values overlap and conflict. The Berkman Klein Center at Harvard has several lessons on privacy included in its database of digital citizenship lesson plans.[3]

These resources and many more, including resources from Common Sense Media, are great - but resources are not enough. We need government to create a cohesive policy that acknowledges that privacy education and protections are essential to children's development and wellbeing. Unfortunately, the U.S. is far behind other countries when it comes to child privacy research and authoritative resources.

Over the past couple years, the UK's Information Commissioner's Office funded research - including interviews with parents and their children - to inform policymaking and create online educational materials built around the questions children kept asking such as "who has my data?" and "what are my rights?"[4] The Irish Data Protection Commission gathered input from students while educating them on privacy, by sending a package of materials to every school that teachers could use to educate their students and send

---

[2] AI + Ethics Curriculum for Middle School, Blakely H. Payne, MIT Media Lab, https://www.media.mit.edu/projects/ai-ethics-for-middle-school/overview.
[3] Digital Citizenship+ Resource Platform, Berkman Klein Center for Internet & Society at Harvard University, https://dcrp.berkman.harvard.edu.
[4] *Children's data and privacy online: Growing up in a digital age. Research findings.*, Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, London School of Economics and Political Science, Funded by the UK Information Commissioner's Office (2019), https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf; *My Data and Privacy Online: A Toolkit for Young People*, Sonia Livingstone, London School of Economics and Political Science, Funded by the UK Information Commissioner's Office, https://www.lse.ac.uk/my-privacy-uk.

feedback to privacy regulators.[5] Similar efforts are underway in multiple countries across the world.

In order to pass evidence-based laws, we need research. Even well-intentioned laws have resulted in unintended consequences. We can mitigate those consequences by consulting with key California stakeholders as well as experts working on these issues around the world. This must include consulting children about their understanding of privacy and their preferences online.

Children spend a significant amount of time at school, and what may work when regulating child privacy at home is often different than in the classroom. In 2014, California led the country in recognizing that nuance as the first state to pass a student privacy law specifically governing edtech companies.

Teachers are a crucial part of this as well. We need to give adults tools and training to implement privacy protections and to model good privacy behaviors. Colleges of Teacher Education rarely offer courses on student privacy or include student privacy concerns in their existing classes, meaning that the vast majority of teachers are never trained on privacy.[6] Strong privacy laws are not effective if people on the ground do not know how to protect data.

It is also essential to examine which protections should be subject to parental consent. Too often, kids get around privacy protections by lying because it is easier than asking their parents, or because they wish to access content without their parent's knowledge (such as LGBTQ support resources or abuse hotlines).

It is important to have fundamental, unwaivable protections - such as a ban on targeted advertising and high privacy settings by default - that keep kids safe no matter what. However, government should respect a parent's judgment about what is appropriate or

---

[5] *Know Your Rights and Have Your Say! Stream Two of the DPC's Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR*, Irish Data Protection Commission (January 28, 2019), https://www.dataprotection.ie/en/news-media/consultations/know-your-rights-and-have-your-say-stream-two-dpcs-public-consultation-processing-childrens-personal; Some Stuff You Just Want to Keep Private: Preliminary report on Stream II of the DPC's public consultation on the processing of children's personal data and the rights of children as data subjects under the GDPR, Irish Data Protection Commission (July 2019), https://www.dataprotection.ie/sites/default/files/uploads/2019-08/Some%20Stuff%20You%20Just%20Want%20to%20Keep%20Private_Consultation%20Report.pdf.

[6] The Case for Including Data Privacy and Data Ethics in Educator Preparation Programs, Ellen Mandinach and Juliana Cotto, Future of Privacy Forum (October 5, 2021), https://studentprivacycompass.org/resource/case-data-privacy-ethics.

inappropriate for their child to access or share. This is where default protections are particularly useful. Children whose parents don't have the time or knowledge to oversee all of their child's digital choices will still have a baseline level of protection. Parents can then have the freedom to make informed decisions to allow their children access to other services or materials.

Everyone wants children to be able to harness the benefits of technology while minimizing risks. Everyone agrees that more needs to be done to accomplish this. California has an opportunity to lead the country on effective, evidence-based child privacy protections and in creating privacy-literate citizens. We must not only protect our children's privacy; we must also inform and educate them so they can protect themselves.

Thank you for inviting me to testify. Please feel free to contact me if you have any questions or need additional information.