Written Testimony of James P. Steyer
CEO and Founder, Common Sense Media

United States Senate Committee on Commerce, Science, and Transportation Hearing
"Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework"
May 1, 2019

Good morning Chairman Wicker, Ranking Member Cantwell, and distinguished Committee Members. Thank you for the opportunity to appear before you, and for your willingness to engage with the complicated--but critically important--issue of consumer privacy.

My name is James P. Steyer and I am the founder and CEO of Common Sense Media. Common Sense is America's leading organization dedicated to helping kids and families thrive in a rapidly changing digital world. We help parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids' lives. Since launching 15 years ago, Common Sense has helped millions of families and kids think critically and make smart, responsible choices about the media they create and consume. Common Sense has over 108 million users and our award winning Digital Citizenship Curriculum is the most comprehensive K-12 offering of its kind in the education field; we have over 700,000 registered educators using our resources in over half of U.S. schools. Common Sense was a sponsor of California's precedent-setting consumer privacy law, the California Consumer Privacy Act (CCPA). We have also sponsored and supported privacy laws across the country and at the federal level, including California's landmark Student Online Privacy Information Protection Act (SOPIPA) and the recently introduced bipartisan COPPA 2.0.

Children And Teens Are Particularly Vulnerable

When we started Common Sense a decade and a half ago, privacy was not a major concern for kids and families. But it has grown significantly as an issue over the past several years, to the point where we find ourselves today. Privacy concerns are particularly acute for kids: Ninety-eight percent of children under 8 in America have access to a mobile device at home.[1] American teens consume an average of 9 hours a day of media,[2] and half of teens report feeling addicted to their devices. Children today face surveillance unlike any other generation – their every movement online and off can be tracked by potentially dozens of different companies and organizations. Further, kids are prone to sharing and impulsive behavior, are more susceptible to advertising, and are less able to understand what may happen to their personal information.[3]

[1] Common Sense: Technology Addiction: Concern, Controversy, and Finding Balance (2016)
[2] Ibid
[3] Children, Adolescents, and Advertising (2006)

Unfortunately, too many companies are not protecting children's and their families' privacy. A recent analysis found that more than half of 6,000 free children's apps may serve kids ads that violate COPPA.[4] 60% of connected devices don't provide proper information on how they collect, use and disclose users' personal information.[5] Millions of kids and parents have had sensitive information--including family chats--exposed by connected toys.[6] Data brokers are selling profiles of children as young as two (and identity theft can occur before a child's first birthday).[7]

A growing lack of privacy and distrust of the online and tech world impacts every family, and could significantly impact the personal development of young people. At Common Sense, we believe kids need the freedom to make mistakes, try new things, and find their voices without the looming threat of a permanent digital record that could be used against them.

It is our goal to help our millions of American members improve the digital wellbeing of their families--and while in many instances that means teaching parents, teachers, and kids good digital citizenship practices and privacy skills, it also means ensuring there are baseline protections in place. Even savvy digital citizens are powerless if they do not know what companies are doing with their information, if they cannot access, delete, or move their information, or if they have no choices with respect to the use and disclosure of their information.

Families' Privacy Expectations And Desires

What do families want in privacy protections? According to our research: More than 9 in 10 parents and teens think it's important that websites clearly label what data they collect and how it will be used.[8] Those same numbers--more than 9 in 10--think it is important that sites ask permission before selling or sharing data.[9] And almost 9 in 10, or 88%, think it is important to control whether data is used to target ads across devices.[10] Speaking of devices, 93% of parents believe that with smart devices it is important to control what information is collected about them and to know when their voices are being recorded.[11]

These views and data points informed the values--including consent, transparency, control, plus special protections for young people--that guided our approach to the privacy work we did in California.

---

[4] Reyes et. al, "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. Proceedings on Privacy Enhancing Technologies (2018)
[5] GPEN Privacy Sweep on Internet of Things (2016)
[6] Jensen, Data Breach Involving CloudPets "Smart" Toys Raises Internet-of-Things Security Concerns, Data Privacy + Security Insider (2017); and Real-World Reasons Parents Should Care About Kids and Online Privacy (2018)
[7] Ibid
[8] Privacy Matters: Protecting Digital Privacy for Parents and Kids (2018)
[9] Ibid
[10] Ibid
[11] Ibid

The California Consumer Privacy Act (CCPA)

The CCPA is the first generally applicable consumer privacy law in America--not limited to financial or health information, or any specific entity--that recognizes that Americans have privacy rights in all of their information, no matter who holds it. Importantly, the California privacy law protects everyone, not just kids or students. This is born of our belief that, while children and teens need special safeguards, the best way to protect them is to have baseline protections for everyone: (1) so families are protected and (2) so businesses cannot pretend they are not dealing with kids.

In California, a statewide ballot initiative focused on notice and saying no to sales of data was the catalyst that led to larger discussions to develop more comprehensive privacy legislation. At Common Sense, we worked hard to expand substantive rights under the law--including opt-in rights (which we achieved for minors under 16), and new access, deletion, and portability rights. The CCPA ultimately passed unanimously through both houses of the California legislature.

The law goes into effect in 2020, and will allow California residents to access the personal information companies collect about them--as well as port their data to another platform, or demand the deletion of their data (with exceptions) if they wish. Californians will be empowered to tell companies to stop selling their personal information. And kids under 16 or their parents must actively consent before their data is ever sold. The Attorney General is charged with enforcing violations of the law--with a private right of action for certain data breaches--and the law applies equally to service providers, edge companies, and brick and mortar entities.

Any Federal Law Should Build Upon California

Like the CCPA, any federal law must go beyond "consent", and include rights to access, port, and delete information. It must enable consumers to say no to the sharing of their information, and it would be even better if the law required that consumers say yes before their information is sold or shared--families would be better served if the rule for all people, not just minors under 16, was that companies could not sell information without opt-in approval. Indeed, the California law is a huge step forward, but it is not perfect and it does not offer consumers all of the protections they deserve. As this committee considers bipartisan federal legislation, additional protections families want and deserve include: the rights to limit companies' own use of consumer information; the ability for consumers to enforce their own rights in court; and the assurance that companies are building default privacy protections (privacy by design) and practicing data minimization. Certain practices should be off limits, and individuals, especially children, should not be able to consent to them (such as, for example, manipulative user designs that subvert user autonomy, or behaviorally targeted marketing to kids).

Privacy protections must be strong across the board, but they must recognize the unique vulnerabilities of children and teenagers. The bipartisan COPPA 2.0 offers an excellent example

of the protections young people need: in addition to putting families in the driver's seat regarding information collection, use, and disclosure, COPPA 2.0 contains additional safeguards (and, for young children, flat prohibitions) around targeted and behavioral marketing; it would enhance the privacy and security of vulnerable connected devices families are bringing inside their homes; and it offers new resources and authority to the Federal Trade Commission to focus on examining the industry and enforcing these protections.

Any law Congress passes should be at least as strong, if not stronger, than California's CCPA. The CCPA will go into effect next year, and it is clear from polling that vast majorities of Californians from all parties support it.[12] What's more, it is also clear from other states that individuals and state legislators are not going to accept laws that are weak on privacy.

And, as with past federal privacy laws, national legislation should ensure that there are baseline protections in place, but provide room and space for states to continue to innovate. A weak preemptive law would be a travesty of justice and take away rights from millions of consumers, not just the eighth of the country that lives in California but the many individuals who live in other states with strong privacy laws such as Illinois, with its biometric law, or Vermont, with its data broker registry.

States have always been the first line of defense to protect individual citizens from scams and unfair business practices, and state tort law has protected the privacy of homes and persons. State innovation in the privacy sphere has brought us data security rules, laws applying directly to ed tech vendors, laws protecting the privacy of our bodies, and laws shining light on data brokers. The speed of technology is lighting fast, and states are in a position to act nimbly and innovate, just like businesses. States are true laboratories of democracy, and in the past few decades they have been engaging on privacy and working with consumers and businesses to determine workable new protections and safeguards.

Any Law Must Be Coupled With Consumer Education

It is critical that any new law be coupled with effective consumer education. From our research at Common Sense, we know that families crave better privacy protections. We also know that some are taking measures to try and protect themselves--for example, 86% of parents and 79% of teens have adjusted privacy settings on social media sites.[13] But in many instances, families have the desire but lack the knowledge. In discussing connected devices with parents, we learned 71% would like to limit data collection, but a full third do not know how.[14]

[12] California Voters Overwhelmingly Support Stronger Consumer Privacy Protections (2019); and Privacy Matters: Protecting Digital Privacy for Parents and Kids (2018)

[13] Privacy Matters: Protecting Digital Privacy for Parents and Kids (2018)

[14] Ibid

This is why it is important to have companies build products, platforms and services with the most protective privacy defaults possible. It is also why kids and adults need to know how to exercise their privacy rights. Education is imperative in this regard. As I mentioned, Common Sense is committed to giving parents and teachers the information they need to make informed choices about the apps they use with their children at home and the learning tools they use with students in the classroom. We provide expert advice articles and privacy evaluations for parents to learn more about how they can protect their kids' privacy and we empower schools and districts to thoroughly assess technology products used in K–12 classrooms. We collaborate with hundreds of school and district partners and provide assistance to software developers to make sure their privacy practices are transparent and comprehensive and created with kids' best interests in mind. We also provide a high-quality Digital Citizenship Curriculum for school communities that supports teachers with improved classroom tools, and prepares kids to take ownership of their digital lives.

At present, across the country, opportunities to empower individuals to make real decisions or protect their privacy are few and far between. Companies offer a "take it or leave it" framework that, because of jobs, school requirements, or an interest in participating in democratic life, individuals feel forced to accept. We must ensure consumers have default protections in place, and we must also work to educate them about additional, or alternative, choices. Digital citizenship education should be a part of school curriculums, and requires more support and funding.

What's more, privacy protections are just one piece of the puzzle. As young people live more and more of their lives online, they face an ever expanding array of opportunities and risks. In addition to protecting children and families' privacy, we must endeavor to provide all kids with access to high quality content, and protect them from being exposed to the worst of humanity with the click of a button, scroll of a feed, or failure to stop a new video from autoplaying. We must consider, as a country, whether laws like Section 230 are serving the best interest of our children, and what we can do to improve the entirety of their digital experience.

Conclusion

Thank you again for your bipartisan efforts to address consumer privacy. It's critical that we teach individuals how to protect themselves, but the burden should not fall entirely on consumers, especially on kids and families. We have seen many businesses will not protect consumer privacy on their own. We need a strong federal baseline privacy law, that offers everyone protections and recognizes the special vulnerabilities of children and teens.