**Prepared Statement of Ariel Fox Johnson**
**Senior Counsel, Policy & Privacy, Common Sense Media**

**First Hearing on Protecting the Privacy of Vermonters**

**Burlington, VT**
**August 6, 2018**

Thank you Attorney General Donovan for arranging this important discussion on how to protect the privacy rights of Vermont citizens and families.

My name is Ariel Fox Johnson and I am here representing the national kids and families organization Common Sense Media, which was a sponsor of California's precedent-setting consumer privacy law, the California Consumer Privacy Act (CCPA). Previously, we spearheaded California's Student Online Personal Information Protection Act (SOPIPA), which was the first edtech vendor focused privacy law in the country. Thank you for the opportunity to speak today.

The CCPA is the first generally applicable consumer privacy law in America--not limited to financial or health information, or any specific entity, but recognizing that Americans have privacy rights in all of their information, no matter who holds it. This information is being collected, used, and shared in unprecedented and unexpected ways. As you consider approaches to protecting the privacy and data security of Vermonters, we urge you to pass broad-based protections that are at least as strong as or stronger than those in California, as well as continue to target especially concerning sectors such as the edtech industry.

Privacy rights are critical for consumers with respect to all manner of companies--while data brokers are certainly among the most opaque actors, and we applaud Vermont's attention to that issue, many companies that consumers interact with directly also collect, sell, and share information in ways consumers do not expect or understand. (Indeed, a poll we conducted this summer found that only a third of teenagers and only a quarter of parents think social media sites and apps do a good job of explaining what they do with users' data.[1] )

Over the next year, legislators around the country will consider and set privacy rights and standards. Given Vermont's history of thoughtful legislation in this area and the well-planned process to discuss these issues already in place, we believe that Vermont can play a significant

[1] *See* Common Sense and Survey Monkey Poll (2018), available at https://www.commonsensemedia.org/about-us/news/press-releases/common-sense-and-surveymonkey-poll-finds-privacy-matters-for-parents.

role in developing, nuancing, and refining standards to protect privacy, especially the privacy of children and teenagers.

## Children And Teens Are Uniquely Vulnerable

Ninety-eight percent of children under 8 in America have access to a mobile device at home.[2] Half of teens say they feel addicted to their mobile devices,[3] and those teens overall consume an average of nine hours a day of media.[4]

It's not hyperbole to say that 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. Young people will spend their entire lives connected in order to get an education and participate in modern society. Further, kids are prone to sharing and impulsive behavior, more susceptible to advertising, and less able to understand what may happen to their personal information. Unfortunately, as a recent Fordham study confirmed--this information is collected, sold, and repackaged, for kids at least as young as 2.[5] Vermont's data broker law targets repackagers and resellers. But we also have concerns about the companies that collect this information in the first place.

Many of these companies come into contact with kids in schools. Education technology providers collect massive amounts of sensitive data about students – including performance records, online activity, health information, biometrics, behavior and disciplinary records, eligibility for free or reduced-price lunch – even cafeteria selections, and whether or not students ride the bus to school. And this information is at risk.

A recent Common Sense evaluation of the privacy policies of the top 100 edtech products found products may be inappropriately using students' information for advertising, selling it to third parties, or otherwise failing to respect it. For example, 38 percent of educational technologies evaluated indicate they may use children's personal and nonpersonal information for third-party marketing and 37 percent indicate collected information can be used by tracking technologies and third-party advertisers. Half indicate they may allow children's information to be made publicly visible.[6]

---

[2] The Common Sense census: Media use by kids age zero to eight (2017), available at https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2017

[3] Common Sense: Technology Addiction: Concern, Controversy, and Finding Balance (2016), available at https://www.commonsensemedia.org/research/technology-addiction-concern-controversy-and-finding-balance.

[4] The Common Sense Census: Media use by teens and tweens (2015), available at https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens.

[5] Fordham Clip: Transparency in the Marketplace for Student Data 2014-2018 (2018), available at https://www.fordham.edu/info/23830/research/10517/transparency_and_the_marketplace_for_student_data/1.

[6] 2018 State of EdTech Privacy Report, Common Sense Privacy Evaluation Initiative, available at https://www.commonsense.org/education/sites/default/files/tlr-blog/cs-state-of-edtech-privacy-report.pdf.

This use of student information is directly contrary to parents' desires. A national poll found that 90 percent of adults – whether parents or not – are concerned about how non-educational interests are able to access and use students' personal information. Eighty-six percent agree that protecting children's safety and personal information should be the No. 1 priority.[7]

Our kids are uniquely vulnerable to privacy harms. Indeed, Vermont has recognized the particular susceptibility of children already--your data broker law contains additional safeguards and disclosure requirements when minors' information is involved.

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. They deserve a world in which their daily musings to friends are not assessed by corporations looking to turn a profit or by nefarious actors looking to manipulate their behavior.

It is our goal to help our tens of 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 hygiene practices and skills, it also means ensuring there are baseline protections in place. Even extremely 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. And an individual has no ability to prevent a corporate or government data breach.

**The California Consumer Privacy Act Provides Important Baseline Protections**

Recently we asked parents across the country how they want to protect their privacy rights, and what tools would help their families. Ninety-four percent of parents think it is important that sites notify them about what data is being collected. The majority of teens (69 percent) and parents (77 percent) say it is "extremely important" for sites to ask permission before selling or sharing their personal information. Eighty-two percent of parents and 68 percent of teens are at least "moderately" worried that social networking sites use their data to allow advertisers to target them with ads.[8] These views informed the values--including consent, transparency, and control--that guided our approach in California.

---

[7] *See* Press Release, *National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared* (2014), available at http://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern.

[8] *See* Common Sense and Survey Monkey Poll (2018), available at https://www.commonsensemedia.org/about-us/news/press-releases/common-sense-and-surveymonkey-poll-finds-privacy-matters-for-parents.

In California, the statewide ballot initiative process drove the legislation. A privacy 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 California Consumer Privacy Act 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-- and port their data to another platform, or demand the deletion of their data (with exceptions) if they wish. Californians can tell companies to stop selling their personal information. And kids under 16 or their parents must opt in before their data is ever sold. The Attorney General primarily enforces 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.

**Vermont Should Enact Strong Baseline Protections & Sector-Specific Measures As Needed**

The CCPA is a good first step, but consumer privacy protections could be stronger. We and other consumer groups are also interested in seeing inclusion of minimization of data collection and use and ensuring that discriminatory financial practices are sufficiently prohibited. We will also face a series of amendments proposed by various lobbies that aim to weaken the legislation now that the initiative is off the table. At the same time, we expect additional and more focused bills regarding emerging technologies such as connected devices and facial/voice recognition.

Vermont can act to protect privacy for all Vermonters. Common Sense recommends the following three strategies/priorities:

1. Enact a broad-based consumer privacy bill that is at least as strong as or stronger than California's.
2. Protect student privacy as a next step, following the SOPIPA model--clear rules of the road to ensure that schoolchildren's information is not exploited for commercial purposes and stays out of the wrong hands. Under SOPIPA, which has been widely acclaimed as one of the most comprehensive student privacy laws of the 21st century, K-12 websites, online services, and mobile applications are prohibited from using students' personal information for targeted advertising or commercial profiling; prohibited from selling students' personal information; and prohibited from disclosing it except in certain circumstances. There are also reasonable security requirements. Notably, SOPIPA is also carefully drafted to help foster innovation and research, so industry may improve educational products and provide customized and digital learning for students.
3. Vermont could take steps to ensure privacy continues to be protected for future generations by enshrining a right to privacy in its Constitution. Only 10 states around the

country expressly recognize an individual right to privacy in their constitutions.[9] We hope Vermont will join them, although we understand this will be a multi-year process. We believe any amendment should acknowledge that privacy is essential to a free and democratic society, encourage affirmative steps to protect privacy, and recognize the unique vulnerability of young people.

Finally, speaking to a central question posed for today's hearing, Common Sense encourages Vermont to designate a Chief Privacy Officer. Seven states currently have a Chief Privacy Officer (and many more have Chief Data Officers). The first CPO was hired in 2003, demonstrating there is increasing recognition of the importance of this position.[10] A high-level, dedicated, and accountable privacy professional serving the interests of Vermonters could help lead the public conversation on protecting privacy rights online and off, focus enforcement efforts, and guide the development of strong and detailed laws and regulations. We believe the overwhelming and growing public concern about this complex issue demonstrates the need for such a figure.

The right to privacy is a fundamental American right. We are grateful for your commitment to protect it. Thank you for your time and we look forward to working with you throughout this process.

[9] *See* National Conference of State Legislatures, Privacy Protections in State Constitutions (2017), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[10] LaHucik, K. Help Wanted: States Hires Pros to Manage, Protect Data, Bloomberg Law (Aug. 4, 2018), available at https://www.bna.com/help-wanted-states-n73014481427/.