

April 7, 2021

Senate Committee on Education
Senator Michael Dembrow, Chair
Senator Chuck Thomsen, Vice-Chair

The Future of Privacy Forum (FPF) writes to share our thoughts on Senate Bill 594. We commend the Oregon legislature's attention to student privacy, particularly student monitoring, and we understand the desire of the legislature to limit monitoring that goes too far. However, as currently drafted, the bill may conflict with federal law and cause significant confusion for school districts. We recommend that the Oregon Senate:

1. Narrow the scope of Senate Bill 594 to prohibit monitoring for specific purposes, which will avoid broadly prohibiting much-needed technology, including assistive technology;
2. Clarify that Senate Bill 594 would not preempt monitoring required by the federal Children's Internet Protection Act (CIPA); and
3. Update the bill to create a council or working group to investigate how Oregon schools utilize student monitoring software and provide recommendations to the legislature.

These changes could help clarify the bill's scope, ensure the bill does not conflict with federal law, reduce confusion for school districts throughout the state, and ensure that the legislature continues to address the evolving needs of Oregon students.

FPF is a nonprofit organization based in Washington, D.C. that focuses on how emerging technologies affect consumer privacy.¹ FPF works closely with stakeholders from practitioners and advocates to policymakers, providing technical assistance, resources, trend analysis, and training. FPF routinely provides expert testimony and comments to the U.S. Congress, federal agencies, U.S. state legislatures, and legislatures around the world.² FPF's Youth & Education Privacy program works to protect child and student privacy while allowing for data and technology use that can help young people learn, grow, develop, and succeed. Amelia Vance, Director of FPF's Youth & Education Privacy program, is an expert on student monitoring and privacy; in addition to writing "School Surveillance: Consequences for Equity and Privacy,"³ Vance was invited to present before the Connecticut General Assembly's Commission on Women, Children, and Seniors Working Group, where they specifically explored "Search and Seizure of

¹ The views herein do not necessarily reflect those of FPF's supporters or Advisory Board.

² Amelia Vance, *FPF Testifies Before Congress on Promoting and Protecting Student Privacy*, Future of Privacy Forum, (May 17, 2018), <https://fpf.org/2018/05/17/studentprivacycongressionalhearing/>; Federal Trade Commission, *The Future of the COPPA Rule: An FTC Workshop*, FTC, (Oct. 9, 2019), <https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop>; Federal Trade Commission, *Student Privacy and Ed Tech*, FTC, (Dec. 1, 2017); Commission on Evidence-Based Policymaking, *The Promise of Evidence-Based Policymaking: Report of the Commission on Evidence-Based Policymaking*, App. G 310, (2017); Amelia Vance, *FPF Letter to NY State Legislature*, Future of Privacy Forum, (June 17, 2019), <https://fpf.org/2019/06/17/fpf-letter-to-ny-state-legislature/>; Liron Tzur Neumann, *Legislating Online Conference – The Knesset, Israel Parliament*, Israel Tech Policy Institute, (Oct. 24, 2018), <https://techpolicy.org.il/blog/legislating-online-conference-the-knesset-israel-parliament/>.

³ Amelia Vance & J. William Tucker, *School Surveillance: The Consequences for Equity and Privacy*, NASBE Education Leaders Report, (October 2016), <https://eric.ed.gov/?id=ED582102>.

Students Personal Electronic Devices.”⁴ Vance also testified on these issues before the Federal School Safety Commission.⁵ FPF regularly convenes a coalition of education, civil rights, and disability rights organizations (including organizations like the National PTA, AASA, the School Superintendents Association, and the Southern Poverty Law Center) to address the privacy and equity problems that can arise from student monitoring initiatives resulting in, among other resources, consensus student privacy principles on school safety and equity.⁶

We commend the Oregon legislature’s demonstrated attention to student privacy. FPF opposes widespread student digital surveillance efforts that risk criminalizing and stigmatizing students, which we’ve written extensively on⁷ in letters to both the Florida Governor and New York legislature.⁸ However, we fear that the current language of Senate Bill 594 may not adequately meet the legislature’s goals, since it is likely to directly conflict with federal law and its broad language is likely to cause significant confusion for school districts across the state.

Recommendation 1: Narrow the scope of the bill to prohibit monitoring for specific purposes.

We recommend that the legislature narrow the bill’s scope and redefine “monitoring software” to include specific types or uses of monitoring software. If the Oregon legislature is explicitly seeking to ban certain technologies that can monitor a student’s physical characteristics, such as facial recognition technology, we recommend amending the definition of monitoring software to reference those technologies directly. Limiting the bill’s scope would help reduce confusion for school districts.

Rather than explicitly prohibiting monitoring technology that can cause students harm, the current definition of monitoring software can be interpreted to apply to a wide range of use cases, which may unintentionally prohibit schools from using certain beneficial technologies. In addition to the need to monitor school networks and devices to ensure compliance with CIPA, detailed below, most schools rely on monitoring software as defined in Senate Bill 594 for essential services such as assistive technologies to help students with certain disabilities.⁹ In an extreme example, the current language can also be interpreted to prohibit schools from using any technology capable of accessing a user’s fingerprint to unlock a device, a standard feature on many computers and

⁴ Connecticut General Assembly, *Connecticut Commission on Women, Children and Seniors: Search and Seizure of Students Personal Electronic Devices Work Group*, (September 17, 2018), <http://ct-n.com/ctnplayer.asp?odID=15611>; H.B. 5170, 2018 Leg. Sess. (Conn. 2018).

⁵ Sara Collins, Tyler Park, & Amelia Vance, *Ensuring School Safety While Also Protecting Privacy: FPF Testimony Before the Federal Commission on School Safety*, Future of Privacy Forum, (June 6, 2018), <https://fpf.org/blog/ensuring-school-safety-while-also-protecting-privacy-fpf-testimony-before-the-federal-commission-on-school-safety/>.

⁶ Sara Collins & Amelia Vance, *40 Organizations Release Privacy Principles for Student Safety*, Student Privacy Compass, (March 16, 2019), <https://studentprivacycompass.org/schoolsafetyprinciples/>.

⁷ *A Closer Look: Network Monitoring*, Student Privacy Compass, (October 23, 2019), <https://studentprivacycompass.org/closerlook1/>; *A Closer Look: Social Media Monitoring*, Student Privacy Compass, (October 30, 2019), <https://studentprivacycompass.org/closerlook2/>.

⁸ Amelia Vance, *FPF Letter to NY State Legislature*, Future of Privacy Forum, (June 17, 2019), <https://fpf.org/2019/06/17/fpf-letter-to-ny-state-legislature/>; and Amelia Vance, *Education, Privacy, Disability Rights, and Civil Rights Groups Send Letter to Florida Governor About Discriminatory Student Database*, Future of Privacy Forum, (July 9, 2019), <https://fpf.org/blog/education-privacy-disability-rights-and-civil-rights-groups-send-letter-to-florida-governor-about-discriminatory-student-database/>.

⁹ Understood, *Assistive technology basics*, (Accessed April 5, 2021) <https://www.understood.org/pages/en/school-learning/assistive-technology/assistive-technologies-basics/>.

devices. Additionally, the bill could also create significant confusion for school administrators that rely on monitoring technology to keep students on task,¹⁰ avoid cybersecurity risks,¹¹ and identify instances of cyberbullying.¹²

We have seen several instances where broad language in well-intended student privacy legislation creates significant confusion in practice.¹³ For example, New York legislators enacted a moratorium on school use of biometric identifying technology, but did not anticipate that the bill's broad scope would prohibit schools from conducting fingerprinted background checks on prospective employees.¹⁴ They had to amend the law almost immediately after its passage to allow that use. Clarifying the scope of Senate Bill 594 would help reduce confusion for school districts and ensure the continued use of beneficial technology.

Recommendation 2: Clarify that Senate Bill 594 would not preempt federal monitoring requirements.

As written, Senate Bill 594 would likely directly conflict with the CIPA.¹⁵ CIPA requires schools subject to the law to filter and monitor students' online activity to prevent them from accessing inappropriate content online. In direct conflict, Senate Bill 594 would prohibit school districts from authorizing or using monitoring software. If enacted as written, school districts across the state would risk losing much-needed federal E-Rate funding.

CIPA applies to schools and libraries that receive federal E-Rate discounts for Internet access, including almost every public school in the country. School districts must file a CIPA certification of compliance with the Federal Communications Commission (FCC). Failure to comply with CIPA would require school districts to reimburse any funding received as a part of an E-Rate grant. According to the Oregon Department of Education, "E-Rate program funding commitments bring an additional \$15-25 million to Oregon schools to support Internet access."¹⁶ If enacted as written, this bill would place that E-Rate funding at risk.

¹⁰ Ali Tadayon, *Teachers grapple with how to keep track of students during distance learning*, EdSource, (May 11, 2020), <https://edsources.org/2020/teachers-grapple-with-how-to-keep-track-of-students-during-distance-learning/631189>

¹¹ Mark Lieberman, *4 Big Cybersecurity Priorities for Schools: Training, Purchasing, Monitoring, and Budgeting*, EdWeek, (March 17, 2020), <https://www.edweek.org/technology/4-big-cybersecurity-priorities-for-schools-training-purchasing-monitoring-and-budgeting/2020/03>

¹² Notar, Padgett, & Roden, *Cyberbullying: Resources for Intervention and Prevention*, Universal Journal of Educational Research, (2013), <https://files.eric.ed.gov/fulltext/EJ1053892.pdf>

¹³ Jules Polonetsky & Amelia Vance, *Student privacy and the law of unintended consequences*, The Hill, (January 18, 2019), <https://thehill.com/opinion/technology/425946-student-privacy-and-the-law-of-unintended-consequences>;

Amelia Vance & Casey Waughn, *Student Privacy's History of Unintended Consequences*, Seton Hall Legislative Journal: Vol. 44: Iss. 3, Article 4, (2019), <https://scholarship.shu.edu/shlj/vol44/iss3/4>.

¹⁴ Anisha Reddy, Jim Siegl, & Casey Waughn, *New York Hits Pause on Biometric Technology in Schools: What it Means for Education Stakeholders*, Student Privacy Compass, (February 8, 2021), <https://studentprivacycompass.org/new-york-hits-pause-on-biometric-technology-in-schools-what-it-means-for-education-stakeholders/>.

¹⁵ 47 U.S.C. § 254.

¹⁶ Oregon Department of Education, *State E-Rate Program and Broadband Connectivity*, (Accessed March 25, 2021), <https://www.oregon.gov/ode/schools-and-districts/Pages/State-E-Rate-Program-and-Broadband-Connectivity.aspx>

CIPA directs schools to develop internet safety policies that include technological measures to facilitate “monitoring the online activities of minors.”¹⁷ As such, school districts comply with CIPA by using monitoring software to monitor students’ online activity. Absent further guidance from the FCC, student monitoring software will likely remain a core element of school district CIPA compliance. Senate Bill 594 would prohibit school districts from authorizing or using monitoring software that would “enable a person to obtain information about another person’s computer activities or computer usage based on the physical characteristics or movements of the computer user”; this would likely be in direct conflict with CIPA’s requirements. As discussed above, the “movements” of the user could be interpreted to include what the user types, clicks, or otherwise interacts with as they engage with a computer. To ensure that Senate Bill 594 does not preclude Oregon school districts from receiving essential E-Rate funding, we recommend that the legislature explicitly clarify that the bill cannot be construed to prohibit schools from monitoring required by CIPA.

Recommendation 3: Commission a council or working group to investigate how Oregon schools utilize student monitoring software and provide recommendations to the legislature.

Finally, we urge the Senate to convene a council or other legislative body to study and develop a strong understanding of how Oregon schools currently use student monitoring technology. Increasingly, schools have adopted monitoring technology in an attempt to identify students who may pose a threat to the school community or students at risk of self-harm or suicide, even though these use cases are not supported by independent evidence or research.¹⁸ Monitoring for these purposes can also risk criminalizing or stigmatizing students,¹⁹ which in turn risks students and parents feeling reluctant to disclose disabilities and receive the accommodative services that could help students succeed.

By commissioning a council or working group to investigate Oregon’s current student monitoring landscape, the legislature will be better able to understand where schools and districts require resources, guidance, and best practices. Importantly, studying student monitoring will help the legislature propose additional laws in the future that can strategically ban problematic or inequitable monitoring while still ensuring that districts are still able to adequately supervise and educate their students.

Thank you very much for your advocacy and support for strong student data protections. Please feel free to contact us if you have any questions or would like additional information.

Sincerely,
Amelia Vance
Director of Education Privacy, Future of Privacy Forum

Anisha Reddy
Policy Counsel, Future of Privacy Forum

¹⁷ Children’s Internet Protection Act (CIPA), Federal Communications Commission, (Accessed April 7, 2021), <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>.

¹⁸ Lynn Jolicoeur & Lisa Mullins, *To Detect Threats And Prevent Suicides, Schools Pay Company To Scan Social Media Post*, WBUR, March 22, 2018, (Accessed March 25, 2021) <https://www.wbur.org/news/2018/03/22/school-threats-suicide-prevention-tech>

¹⁹ See note 3.