FUTURE OF PRIVACY FORUM

1400 Eye Street NW, Suite 450, Washington, DC 20005 | 202-768-8950 |
fpf.org

To Whom it May Concern:

As the Minnesota House of Representatives considers the Student Data Privacy Act (HF 1507), the Future of Privacy Forum (FPF) is writing with concerns about the proposed language of the bill, which would create conflicting requirements for schools and education technology companies, and likely cause unintended consequences for Minnesota schools and students. These concerns include:

- Inconsistent definitions in the Student Data Privacy Act versus the federal student privacy law, FERPA;
- Potentially increasing the likelihood of data breaches by requiring companies to publicize their security practices and procedures; and
- Students missing out on important educational programs and services due to opt-out requirements.

FPF has been working on student privacy for four years. Among other accomplishments, we jointly created the Student Privacy Pledge with the Software and Information Industry Association (a voluntary and legally binding promise by more than 300 Ed Tech companies regarding the handling of student data); have read or provided comments on the more than 600 student privacy bills introduced in 49 states since 2014 and the eight federal bills introduced in 2015; released numerous resources on student privacy, including a guide for de-identifying student information under FERPA; and created FERPA|Sherpa, a website compiling education privacy resources and tools with sections aimed at parents, schools, service providers, and policymakers. We work frequently with all of the relevant stakeholders in the student privacy realm, from districts and ed tech providers to parents and policymakers.

We appreciate your important work on student privacy. As we all seek to provide appropriate protections for student data, we should ensure that the benefits of technology are maximized for students and their learning outcomes, while protecting existing beneficial programs and uses.

Some of the key definitions in this bill, such as the definitions for "education data," "technology provider," and "student," do not align with the Family Educational Rights and Privacy Act (FERPA) definitions for those terms. The broad definition of "educational data" as "data which *relates* to a student" will likely be difficult for schools and companies to interpret, rather than a more targeted definition which would specifically address the kind of personal information this bill is intended to protect, such as "data which may directly or indirectly identify a student." The lack of consistency with federal definitions may also cause confusion as Minnesota schools attempt to reconcile multiple standards. Overbroad definitions can also have the unintended consequence of preventing legitimate and beneficial uses of student data, such as Louisiana's 2014 student privacy law, which confused both educators and administrators and led to schools that were afraid to announce student athletes' names at games, hang student artwork in the hallway, or have yearbooks.

Other requirements in the bill may also have unintended privacy, security, and administrative consequences for student data. The prohibition on using educational data for "any commercial purpose" has a laudable intent, but would have the practical effect of banning important educational services, such as school photos, tutoring services, and sharing scholarship opportunities.

Requiring companies to make the details of their security practices and procedures available as public data could provide bad actors with the means to game security protocols, putting student data at additional risk. Logging provisions that require technology providers to attach an individual employee or student name to access records may require significant and expensive development efforts for some technology providers, particularly new small businesses. In addition, requiring these logs to be made public with individual names attached, instead of persistent identifiers, may also contradict existing privacy laws or employment contracts. At the end of the day, companies, not their individual employees, should be held accountable when there is inappropriate access to student data.

The requirement that parents be able to opt-out is also likely to create unintended consequences for parents, students, and schools, as it outsources vetting obligations to parents who may not be the best to evaluate the technical nuances or legalese of a privacy policy. This can also cause parents to unintentionally exclude their children from receiving critical education services. Allowing parents to opt-out makes it difficult for schools to do everything from improving instruction, scheduling bus services, and sending a student's transcripts to colleges. This is also an equity issue; if an ed tech product is not safe to use in schools, the answer is not to allow an opt-out, but to use a different product. Students whose parents are not as engaged should not be less safe than their peers.

Finally, without providing additional resources for Minnesota schools to train educators and administrators on the law's requirements, the law is unlikely to be implemented with fidelity and student privacy will likely continue to be at risk, as between seventy and ninety-five percent of all inappropriate data disclosure occurs due to human error.

We recommend that any student privacy legislation adopt common sense standards that ensure that the benefits of educational data and technology can be harnessed responsibly. Schools are in the best position to provide effective protections for their students' information when privacy and security requirements are clear and are crafted so as not to create conflicting obligations or unintended consequences. Many states have achieved these goals in their student privacy laws; in particular, Georgia's Student Data Privacy, Accessibility, and Transparency Act, passed in 2015, has been upheld as a model, achieving the ideal balance between protecting student privacy while still allowing for the important uses of data and technology that can help students succeed.

Thank you very much for your advocacy and support for the strong protection of student data. Unfortunately, we believe that this bill as written would cause undue harm rather than providing an appropriate privacy and security framework that also allows for the best learning outcomes. 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