Faith Boninger Testimony re H.650, February 6, 2026

Chair Marcotte and members of the committee:

Thank you for the invitation to testify today about H.650.

My name is Faith Boninger. I'm testifying today in my personal capacity, but for identification purposes, I am a research faculty member at the University of Colorado Boulder, in its School of Education's National Education Policy Center. I've studied marketing in schools for nearly 20 years, and for the past ten years, my research has focused on the educational and privacy impacts of the digital technologies used in schools. I don't accept funding from tech companies for my work.

I very much support H.650 as essential to protecting Vermont's children—including their data privacy, the integrity of their educations, and the content they're exposed to online through their schooling.

Ubiquity and Nature of Digital Educational Products

Schools are so different than when we—or even our children—were kids. Digital educational products are now ubiquitous in American classrooms. For those of us regularly in schools, their ubiquity can make it hard to remember that it was not always like this. For those of us not regularly in schools, it's hard to comprehend all the many functions that digital educational products serve, and also shape. Any given district may use hundreds of digital products, or more.[1] Teachers and students use them to organize and provide curriculum content, structure classroom teaching and student collaborations, assess and track student learning, and communicate with parents and guardians. Administrators use them to make staffing and procurement decisions, and for reporting purposes. Just a handful of student-facing examples are Google Workspace for Education, Kahoot!, Zearn, Khan Academy, MagicSchool, Nearpod, and PowerSchool.

Some argue that, used under the supervision of teachers for educational purposes, so-called "ed tech" is different, and better, than other forms of digital technology platforms like social media or videogames. My research indicates that this isn't true. In many ways, ed tech is worse. This committee has spent a lot of time thinking about big tech, data privacy, and age-appropriate design of tech products. Everything you know from those deliberations is relevant to thinking about digital products used in schools. Essentially, ed tech is still *big tech*—complete with many

[1] Instructure reports that in the 2023-24 school year, school districts it works with accessed an average of 2,739 distinct ed tech tools annually.
Instructure (2024). *EdTech top 40: A look at K-12 edtech engagement during the 2023-24 school year.* Salt Lake City, UT: Instructure. Retrieved May 5, 2025, from https://www.instructure.com/edtech-top40

of the design concerns associated with the social media and gaming platforms that kids use outside of schools. And then some, because "ed tech" products are mediating between teachers and students, delivering educational content, making educational decisions, and through all of it, collecting huge amounts of sensitive data from children as they learn and grow. Importantly, children are required to use these products in their schooling.

Pedagogical Issues to Consider

Digital products influence the nature of teaching and learning in a variety of ways.[2] All of them point to the importance of the state knowing which products are being used in its schools, establishing a means of understanding what their characteristics are, and laying out ground rules for companies that want to do business in Vermont and have access to its children. Particularly, the pedagogical theories embedded in digital platforms and learning programs shape the student learning environment. In other words, the algorithms embedded in these products shape teaching, curriculum, and assessments. They tend to narrow the curriculum to competency-based approaches that are amenable to digital delivery and assessment. They also may embed cultural and other biases in curriculum and in assessments. Further, digital educational products may expose students to marketing and behavioral tracking. This is especially the case for students in low-income districts, which are more likely to choose less costly products or options. Assessments in digital educational products that use predictive analytics, artificial intelligence, and machine learning can harm students in difficult-to-identify ways. As a general rule, the economics of bringing tech products to market incentivizes opacity and discourages adequate testing of their algorithms.

Student Data Privacy

Ed tech products also collect vast amounts of data. They do this partly to fulfill their intended educational functions.[3] And also because more data allows for additional uses, including interoperativity with other products and the development of new features and complementary products.

Importantly, data privacy policies, consistent with most federal and state law, distinguish between "student data" that is clearly associated with a student and "de-identified data" that no longer has that student's identifying information attached to it. There are no retention limits on so-called de-identified data. Providers can save, share, and use these data in perpetuity for all sorts of commercial and other purposes, like predicting the likelihood that a student might

---

[2] Boninger, F. & Molnar, A. (2020). *Issues to consider before adopting a digital platform or learning program*. Boulder, CO: National Education Policy Center. Retrieved February 4, 2026, from https://nepc.colorado.edu/publication/virtual-learning

[3] Access4Learning Community (2024). National Student Data Privacy Agreement, Standard Version 2 (Clauses 4.5-4.7). Retrieved February 3, 2026, from https://files.a4l.org/privacy/NDPA/NDPA_v2-2_STANDARD_WEB.pdf

engage in risky behaviors or commit a crime. And whether the predictions are accurate matters less than that they're made and used, for such uses as determining insurance rates or police surveillance or guiding students toward different academic tracks. In short, providers are enabled to collect, retain, and use data extracted from students from all aspects of their state-required schooling—for their own undisclosed purposes, in perpetuity, with virtually no limits.

Artificial Intelligence (AI)

AI amplifies these concerns. In addition to stand-alone AI products for schools, other ed tech products increasingly incorporate generative AI features. There's a lot of money supporting the integration of AI into public schools, and it's happening at dizzying speed. Products that incorporate artificial intelligence are particularly opaque, as the mathematical calculations embedded in them are unknowable even to their own developers.[4] These products threaten to corrupt curriculum with misinformation, degrade the relationships between teachers and students, bias consequential decisions about student performance, exacerbate violations of student privacy, increase surveillance, and further reduce the transparency and accountability of educational decision-making.[5] All of these, of course, increase the need for the registry provided by H.650. And for annual registration to address the fact that products continually change, with many of those changes currently in the direction of more AI.

Students and Their Schools Need Their State to Support Them

In theory, districts carefully choose the best ed tech products, negotiate contracts with providers, and directly control the ways that the products work.[6] That's not the reality. More often than not, teachers and administrators are flooded with marketing for tech products. Districts lack the personnel, expertise, and power to clarify contract clauses and negotiate effectively with providers. And although they may try products before they adopt them, they can't legally examine the programming of proprietary products, including the programming that determines how a product makes educational decisions and how it processes student data.[7] In many cases,

---

[4] Williamson, B., Molnar, A., & Boninger, F. (2024). *Time for a pause: Without effective public oversight, AI in schools will do more harm than good*. Boulder, CO: National Education Policy Center. Retrieved April 11, 2025, from http://nepc.colorado.edu/publication/ai

[5] Williamson, B., Molnar, A., & Boninger, F. (2024). *Time for a pause: Without effective public oversight, AI in schools will do more harm than good*. Boulder, CO: National Education Policy Center. Retrieved April 11, 2025, from http://nepc.colorado.edu/publication/ai

[6] In 2008 and 2011, U.S. Education Department expanded its definition of "school officials," as used in FERPA, to include "contractors, consultants, volunteers, or other third parties" that perform "an institutional service or function for which the agency or institution would otherwise use employee." Ed tech companies rely on this definition to claim school official status, even though they cannot be "under the direct control of the agency or institution with respect to the use and maintenance of education records," as required.
Privacy Technical Assistance Center, U.S. Department of Education (n.d.). Who is a "school official" under FERPA? Retrieved February 4, 2026, from https://studentprivacy.ed.gov/faq/who-school-official-under-ferpa

[7] For example, Zearn markets itself as providing a comprehensive, standards-aligned K–8 mathematics curriculum. However, it provides no way for educators to review its complete curriculum in detail. The

districts, schools, or teachers adopt products via "click-through" agreements without any negotiation at all. Google, which is a major provider worldwide, as a matter of course dictates terms and conditions to districts that districts have no recourse but to accept. And as with any other digital product, when ed tech products are "updated," schools must either accept the changes or absorb the costs involved in finding alternatives. It's very difficult, if not impossible, for a parent to know which products are used or may be used by their child, or how those products have been vetted.

Small and under-resourced districts have no money to hire enough staff to review and vet products or to pay for adequate data protection. And the more products that are used, the more opportunity there is for data misuse—both by outside "bad actors" and by the providers and the sub-contractors with which they share data. And, again, many districts are currently using hundreds of products. While many districts try to vet products for data privacy concerns, they are limited in their ability to do so.

School leaders—and the children and families affected by directly by the ed tech products they adopt—need higher-level policy to support them by establishing oversight and accountability mechanisms. The registry proposed in H.650 would free districts of the expense and effort required to vet platforms and negotiate with providers. It would also reduce inequities among districts and leverage the power of the state to ensure the quality and safety of the products that students use.

The registry serves both as assurance of the pedagogical quality of products that can be used in the state and also, essentially, as a privacy agreement between the state and providers. It provides a way for the public to know about the products that enter its schools, and to leverage the power of the state to impact the nature of those products. As such, it's an important step in improving the lives of Vermont's children and families.

Suggestions for Revision

The bill as written addresses almost everything my research suggests that it should in order to adequately protect Vermont's children. I do, however, have some suggestions:

1. As written, a certified product will not sell or share data with third parties. In many cases products must share data with sub-contractors in order to function. I recommend adding a

---

platform offers documentation to show that it meets local standards in each U.S. state, but the software prevents independent evaluation of lesson quality, problem sets, or instructional sequences. Most critically, the adaptive algorithms that determine student pathways, prerequisites, and readiness for advancement are "black boxed," making it impossible for educators to assess whether these decisions align with district instructional goals or individual student needs.
Boninger, F. & Nichols, T.P. (2025). *Fit for purpose? How today's commercial digital platforms subvert key goals of public education* (p. 46). Boulder, CO: National Education Policy Center. Retrieved February 4, 2026, from https://nepc.colorado.edu/publication/digital-platforms

provision for this kind of sharing that also holds sub-contractors accountable for the student data that comes into their hands. The bill could require providers to list their sub-contractors and have the sub-contractors register as well. There will be overlap in the sub-contractors used by different providers.

2. As written, the bill does not define "student data." I recommend including a definition that explicitly includes de-identified student data as "student data."

3. As written, the Secretary of State is fully responsible for developing, publishing, and annually reviewing the standards for product certification. It may be more practical to create an independent entity (perhaps under the supervision of the Secretary of State and/or together with the Agency of Education) to conduct these activities. It will be important to include the expertise of educators who can address the products' pedagogical aspects and developers who can define and evaluate issues associated with programming.

Conclusion

Overall, H. 650 is an important step forward in recognizing and reducing the threats posed to Vermont's children by the technology they use in school. I support it wholeheartedly and thank you again for inviting my testimony.