TESTIMONY

Testimony to: Senate Committee on Education

Respectfully Submitted by: Faith Boninger

Subject: H.650 — An act relating to educational technology products

Date: April 19, 2026

Chair Bongartz 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'd like to share with you what I've learned from my research and analysis of the implications of schools' use of digital educational products. My research leads to my assessment that H.650 is an invaluable step forward in protecting Vermont's children—specifically the integrity of their educations, the content they're exposed to online through their schooling, and their data privacy. And then I'll offer some thoughts about specific aspects of the bill.

Ubiquity and Nature of Digital Educational Products

The first thing is that 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. Or that it doesn't have to be. 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—or even thousands—of digital products.[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.

---

[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

Just a handful of student-facing examples are Google Workspace for Education, Kahoot!, 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. Essentially, ed tech is still *big tech*—complete with many 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 now 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 products' algorithms.

Student Data Privacy

Ed tech products also collect vast amounts of data. They do this partly to fulfill their intended educational functions. And also because more data allows for additional uses, including

[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

interoperativity with other products and the development of new features and complementary products.[3]

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 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. 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

---

[3] Boninger, F. & Nichols, T.P. (2025). *Fit for purpose? How today's commercial digital platforms subvert key goals of public education*. Boulder, CO: National Education Policy Center. Retrieved February 4, 2026, from https://nepc.colorado.edu/publication/digital-platforms

[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

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.[6]

In many cases, teachers adopt products via "click-through" agreements without any negotiation at all. Along, Kahoot!, Nearpod, Prodigy, and Zearn are just a handful of products that can be accessed this way. In this common situation, there's no contract. Products that can be obtained for no cost are more likely to be used by financially challenged districts or by teachers without official district support. And "free" products procured via click-through arrangements are more likely to contain advertising to students. Prodigy, for example, contains in-app marketing. Google, which is a major provider worldwide, as a matter of course dictates terms and conditions to districts that districts that use it have no choice 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, how those products have been vetted, or how those products are interacting with their children. Digital products are not like textbooks that are fully transparent for all to see and evaluate.

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, if not more. While many districts try to vet products for data privacy concerns, they are limited in their ability to do so.

The majority of districts in Vermont use a standardized Data Privacy Agreement (DPA) created by the Student Data Privacy Consortium. This DPA is better than many and has some important protections[7], but it was created in partnership with industry consortium members and therefore

---

[6] For example, the product Zearn is marketed 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 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

[7] Including a provision that explicitly holds a buyer of a product to abide by the DPA, detailed definition of "Student Data" and "Educational Records," an option for the Local Education Agency (LEA) to choose to "transfer" as the means by which the provider will eventually dispose of Student Data, and the opportunity for

raises concerns about "the fox guarding the henhouse." Of particular worry to me are provisions that allow providers to de-identify student data and metadata and to retain de-identified data, even after a district stops using a product. De-identification was a real and significant action back when FERPA was enacted, but as I mentioned earlier, in the age of digital platforms, de-identified data are a valuable, fungible commercial asset. The DPA doesn't include a clear retention schedule that determines when student data should be deleted. Importantly, it names providers as "school officials" under FERPA[8], theoretically under the direct control of the school, but unless districts individually negotiate terms that don't appear by default in the DPA, their control is minimal at best.

School leaders—and the children and families affected directly by the ed tech products they adopt—need higher-level policy to support them by establishing oversight and accountability mechanisms. This kind of support isn't inconsistent with local control; it facilitates local control by weeding out the obviously bad players, and by allowing the state to provide local communities with the information they need to decide whether their own self-determined pedagogical goals can be advanced by particular digital products—or not. The registry proposed in H.650 would free districts of the expense and effort required to vet platforms. It would also reduce inequities among districts and enable the state to leverage its power to ensure the quality and safety of the products that students use.

The registry enables the state to certify the quality of products that can be used with Vermont's children. It provides a way for the public, along with schools and districts, to know about and be more confident about the products that enter its schools. It also provides a way for 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.

Specific Considerations

I do, however, have some thoughts about details of the bill as written:

---

the LEA to audit security and privacy measures. In an age where data are easily copied, however, it is unclear that transferred data will not also be copied and de-identified. It also appears that any audit would have to be at the LEA's expense; and it's hard to imagine that audits would include review of proprietary algorithms. Student Data Privacy Consortium (2024). *Standard Student Data Privacy Agreement* (VT-NDPA-V1). Retrieved November 1, 2024, from https://sdpc.a4l.org/agreements/VT_NDPA_V1.pdf [currently unavailable]

[8] 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

1. It isn't clear that filing is annual. That should be made explicit—especially given the fluidity of the education technology market.

2. It's important that persons filing with the state will provide information about all their products, even if they all aren't explicitly being used in Vermont schools at that time and even if they're offered to schools at no cost. As I mentioned earlier, "free" products don't offer the protection of a negotiated DPA and are often the ones that contain advertising and marketing.

3. It remains to be determined how districts will provide information about the products their students are using. You may find that they don't always know. A given district might, for example, have a list of recommended or allowed products but not maintain a list of which ones are actually being used. To the extent this is the case, it convinces me even more of the need for a registry.

4. The report to be produced by the Agency of Education (AOE) will include a determination of whether independent third-party consultants should assist with certification. The bill text references Internet Safety Labs, which can help with data-privacy-related concerns. The AOE might also want to consult with independent experts in its consideration of whether—and how—assistive technology may be included in an Individual Education Plan. Assistive technology is useful in some cases but may be counterproductive in others.[9]

5. The criteria to be considered in the certification process currently include targeted advertising. I recommend expanding this to include, also, advertising that is not targeted.

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. Thank you again for inviting my testimony.

[9] Specific cases that call for assistive technologies include: (1) A nonverbal child that uses an iPad or other computerized speech-generating device to allow them to communicate; (2) A child with hemiparesis that impacts their arm/hand may use speech-to-text because they are unable to physically write/type; (3) A child with dyslexia/vision loss my need access to audiobooks.