INTERNET SAFETY LABS

3146B Sports Arena Blvd #1004
San Diego, CA 92110
(619) 894-9030
internetsafetylabs.org

February 6, 2026

House Committee on Commerce and Economic Development
Rep. Michael Marcotte, Chair and Rep. Edye Graning, Vice Chair

Re: Testimony in Support of the Vermont H.650 – An act relating to educational technology products

Dear Chair Marcotte, Vice Chair Graning and esteemed committee members,

I'm Lisa LeVasseur, founder and research director of Internet Safety Labs, a non-profit, non-partisan product safety testing organization. I'm here today to speak in support of proposed bill H.650. I'm grateful for the opportunity to speak to you today, as we've amassed a sizeable body of work around edtech safety and privacy since our start in 2019.

As a product safety testing organization, we look "under the hood" of technology to assess the riskiness of the *app's* behavior—not the *company's* behavior or what the company says about the app in the privacy policy.

Some of you may be familiar with our work around EdTech. In 2022 we performed the first of its kind safety benchmark to identify privacy risks in edtech used by students in 663 K-12 schools across the US[1]. We published three in-depth reports on the findings as well as more than 1700 mobile app safety labels viewable in our App Microscope[2]. Our safety labels assign an overall privacy risk score and identify the third parties observed to be in communication with the app.

In 2023-2024 we worked with Brigham Young University on a project for the Utah State Board of Education to compare the privacy behavior of 100 apps used in Utah K-12 schools against what the data privacy agreements (DPAs) or privacy policies promised[3]. We continue to systematically measure safety and privacy risks in both web and mobile apps, to produce new and improved safety labels as a public good.

We are in strong support of H.650 as a much-needed step towards edtech product safety accountability. Here are some of our research findings that support the need for greater scrutiny of the technology K-12 students are using.

---

[1] 2022 US K12 EdTech Benchmark Resources, February 4, 2024, https://internetsafetylabs.org/resources/reports/2022-us-k12-edtech-benchmark/
[2] App Microscope safety label viewer: https://appmicroscope.org/
[3] "Utah EdTech App Data Collection and Sharing: 2023-25 Investigation", August 20, 2025, https://www.schools.utah.gov/studentdataprivacy/files/Utah%20EdTech%20App%20Data%20Collection%20and%20Sharing%20-%202023-25%20Investigation.pdf

3146B Sports Arena Blvd #1004
San Diego, CA 92110
(619) 894-9030
internetsafetylabs.org

In our 2022 benchmark, we were able to fully inspect 1,357 apps. 96% of apps were in communication with third party entities. This isn't a particularly alarming or surprising result; it reflects the reality that virtually all apps include third party software components, which means they are sharing student data with 3rd parties.

In the benchmark, we also observed the following:

- 78% of the apps studied communicated with advertising and marketing platforms, allowing these risky third parties to glean data about children.

- Nearly 70% (68%) of apps were in communication with Google servers (even though the sample was a nearly 50/50 split between Apple and Android apps: 51% iOS apps and 49% Android apps).
    - In other words, Apple apps commonly included Google software components, but Android apps never included Apple software components.

- 13% of apps included targeted ads, which, while expressly prohibited by COPPA, still appeared in apps used by school age children, in recommended or required apps by schools.

- COPPA Safe Harbor certification appeared to effectively prevent the presence of targeted ads in certified apps, but it didn't affect the presence of communication to risky adtech and marketing companies.
    - COPPA certified apps had a higher percentage of ads (22%) than the overall sample (15%).
    - 74% of COPPA certified apps scored the highest risk score as compared to 55% of apps in the overall sample.

- Moreover, it's important to recognize that schools legitimately recommend websites and apps that aren't expressly for children. 28% of the apps that were recommended or required by schools were not for children—this included apps like Spotify, Wikipedia, New York Times, Museums, zoos, etc.

- Regarding permissions sought by the apps:
    - 79% of apps requested location information.
        - 100% of Android apps requested location information.
    - 65% of apps requested access to the camera or microphone.

- On average, schools recommended or required 58 apps to students, but only 29% of schools had evidence of vetting these apps, and we only found only 14% of schools afforded parents

3146B Sports Arena Blvd #1004
San Diego, CA 92110
(619) 894-9030
internetsafetylabs.org

or students 18 years or older an opportunity to consent to required technologies. To bring this closer to home:

- In the 13 Vermont schools we audited, closer to 40% of the schools performed technology vetting, and 20% provided an opportunity to consent.
- 69% (9) of the schools sampled in Vermont used the Student Data Privacy Consortium (SDPC) tools to manage technology (a good thing).
  - Bennington Elementary school, one such school using the SDPC tools, was found to have 124 approved technologies listed for the school.
- https://public.tableau.com/app/profile/internetsafetylabs/viz/K-12EdTechBenchmark2022/StateSummary

In the Utah research, 44% of the 100 studied apps collected data not identified in the DPA or the privacy policy. Eleven percent of the apps sent data to third parties not mentioned in the DPAs, and 36% communicated with adtech platforms—even without the visible presence of ads.

All of which is to say, it's high time we systematically screen edtech apps for risky behaviors.

H.650 can go a long way to help mitigate the risks of these typical app behaviors.

First, I want to highlight a particularly good inclusion in the bill's definitions section, namely 2444a.(2): "Provider of an educational technology product". The definition scope includes products that are "in use at a school with or without a contract". This may strike some as overreach, but it is of vital importance. In our 2022 benchmark, we found that only 29% of educational technologies in our sample were licensed by the school or district and 71% of technologies were off-the-shelf.[4] To truly keep students safe from risky software behaviors, we must be concerned with all technologies that schools are recommending or requiring students to use.

Secondly, there is a naturally occurring power and information asymmetry between technology manufacturers and licensees of technology products. Yet we have had edtech manufacturers tell us outright that they are not the data controller and therefore not responsible. They assert that they are merely providing a platform and the schools alone are the data controller, citing Section 230 of the Communications Decency Act (CDA) of 1996. We refer to this as *deliberate data controller confusion* and since 2023 we have advocated that manufacturers of educational technology licensed by Local Education Agencies (LEAs) be regarded as joint data controllers

[4] "2022 K-12 Edtech Benchmark Revisited: Unvetted Off-the-Shelf Apps Outnumber Licensed Apps 2-to-1", August 6, 2025, https://internetsafetylabs.org/blog/research/2022-k-12-edtech-benchmark-revisited-unvetted-off-the-shelf-apps-outnumber-licensed-apps-2-to-1/

3146B Sports Arena Blvd #1004
San Diego, CA 92110
(619) 894-9030
internetsafetylabs.org

along with the LEAs[5]. The LEAs did not write the software, select, or even approve the variety of third-party data processors baked into the product. And, as our research has confirmed, often, the manufacturer doesn't accurately disclose the data processors. In no way can LEAs be conceived of as sole data controllers.

Thirdly, the kind of certification defined in section 2444c (b)(4) of the bill relating to "design features of the product" is very feasible. You may hear from opponents of the bill that such an assessment is too onerous and too expensive—or worse, not possible. I'm here to preempt those arguments with several years of hands-on experience: these kinds of certifications are possible and practical. ISL's current and forthcoming safety labels (available at appmicroscope.org) will address everything listed in this section of the bill and more.

There are, however, some additional items you may like to consider in 2444c(b)(4):

1. Certification should include identifying and minimizing edtech platform communication with advertising and marketing entities (either from the app or backend server-to-server). These adtech and marketing platforms routinely uniquely identify the person (i.e. student) associated with all incoming data packets. Virtually every network communication from a mobile app or unprotected browser allows student identification.
    a. From our 2024 research, we can state definitively that the magnitude of commercial surveillance is staggering. In our report, "The Worldwide Web of Human Surveillance" [6], we identified and researched the beating heart infrastructures that enables commercial surveillance at scale. There is a global, decentralized network of advertising and marketing platforms called customer data platforms (CDPs, like Adobe) and identity resolution platforms (IDRPs, like LiveRamp) that are architected to ingest customer data from disparate sources, associating them to a unique person through "identity resolution" techniques. These platforms aggregate personal information in bulk via application programming interfaces (APIs), and transactionally through digital advertising by the inclusion of proprietary personal identifiers conveyed in the real-time bidding protocol. ISL constantly assesses marketing and adtech platforms and their sites proudly

[5] "Data Controller Confusion in EdTech", May 9, 2023, https://internetsafetylabs.org/blog/insights/data-controller-confusion-in-edtech/

[6] "Worldwide Web of Human Surveillance: Identity Resolution and Customer Data Platforms", July 24, 2024, Internet Safety Labs, https://internetsafetylabs.org/wp-content/uploads/2024/07/Worldwide-Web-of-Human-Surveillance-Identity-Resolution-and-Customer-Data-Platforms.pdf

3146B Sports Arena Blvd #1004
San Diego, CA 92110
(619) 894-9030
internetsafetylabs.org

assert "cookieless tracking", and "personalized experiences for *visitors"*. Note that this is a deliberate word choice; not customers but visitors[7]. We are not anonymous online. Of the combined total of 360 CDPs and IDRPs studied in 2024, only 16.4% of these platforms were registered data brokers, when many more of them should be.[6]

There are two types of commercial surveillance infrastructures: (1) the decentralized one described above that enables entities to share customer data at tremendous scale, and (2) proprietary infrastructures from the Big Tech giants. Both of these infrastructures knit together disparate data sources to develop increasingly invasive and comprehensive profiles of people. Worse, the mechanisms for knitting this data together—especially in the case of the decentralized entities—indiscriminately hoover up the data of everyone, including children. ISL found that 35% of the apps (539 apps) in our 2022 K12 Edtech benchmark sent data to CDPs or IDRPs.[6]

Disturbingly, in our audits over the past few months we are seeing more CDPs and IDRPs in the network traffic of all apps including edtech apps. We are also seeing an increase in adtech and martech platforms internally adding these functions into their services. It starts to look like a worldwide, user-identifying, customer database sharing-a-palooza. In our next version of safety labels we will provide an indication of such high-risk companies found in app network traffic or in SDKs.

b. We are also seeing an increase in the presence of third-party screen and session recording tools in apps, which are used for marketing as well as usability and new feature testing. We currently assess the presence of these tools as high risk particularly due to ubiquitous user identification.

c. Finally, item 2444c(b)(4)(B) "Use of artificial intelligence" needs more specificity. We suggest enumerating specific so-called "AI" technologies such as:
    i. Use of machine learning and large language (or other media) models. Who is the third-party provider of the model? Is student data being used to train the model? Does the app offer a way to disable this behavior?
    ii. Use of chatbots. Who is the chatbot provider? What third parties have access to student prompts? What kinds of guardrails are installed? The Young People's Alliance has proposed banning the use of human-like chatbots for children entirely and has created a strong list of empirically

[7] Here's one example: https://getuntitled.ai/blog/website-visitor-tracking-software/

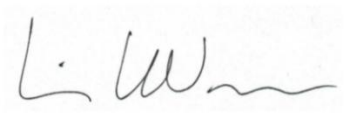
INTERNET SAFETY LABS

3146B Sports Arena Blvd #1004
San Diego, CA 92110
(619) 894-9030
internetsafetylabs.org

measurable chatbot behaviors which constitute human-like behavior.[8] We are adding this into our next version of app safety labels for release mid-year this year.

In conclusion, ISL is pleased to support the novel approach to holding educational technology manufacturers accountable for their products described in H.650, and we stand ready to support the state of Vermont in any way we can.

Sincerely,
Lisa LeVasseur



Executive Director & Research Director
Internet Safety Labs

[8] https://smggrfyky6jfw5l3.public.blob.vercel-storage.com/humanlike-ai.pdf